

世纪本科财经管理类专业实验与实践系列规划教材
丛书主编◎胡巧多

电子支付与信息安全实践教程

主　编◎张新谊
副主编◎叶　龙

清華大学出版社

21世纪本科财经管理类专业实验与实践系列规划教材

丛书主编：胡巧多

电子支付与信息安全实践教程

张新谊　主　编

叶　龙　副主编

清華大学出版社

北　京

内容简介

本书是为高校非计算机专业学生特别撰写的。它结合现场的实验软硬件环境，并充分考虑了学生的培养特点以及将来就业的社会需求，力求让学生通过实验实践，完善电子支付与信息安全的理论学习，更加深入理解电子支付与信息安全的意义和作用。

本书共分8章，分别为操作系统篇、网络系统安全篇、病毒篇、应用安全篇、数据库篇、电子商务应用篇、电子商务环境搭建与营销支付篇和电子商务物流篇，本书还提供了13个实验供学生练习。

真实、体验、直观是本书的特色，通过本书的学习和交流，可使学生在实际环境中动手操作，并从实践中检验知识。

本书既可作为高校非计算机各专业的实验教材，也可作为高职高专各专业的实验教材，还可作为其他专业人员的参考书。

图书在版编目(CIP)数据

电子支付与信息安全实践教程/张新谊主编. --北京：清华大学出版社，2012.7
(21世纪本科财经管理类专业实验与实践系列规划教材)
ISBN 978-7-302-28651-6

Ⅰ. ①电…　Ⅱ. ①张…　Ⅲ. ①电子商务－支付方式－高等学校－教材 ②电子商务－安全技术－高等学校－教材　Ⅳ. ①F713.36

中国版本图书馆CIP数据核字(2012)第077065号

责任编辑：索梅　王冰飞
封面设计：
责任校对：时翠兰
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：10.25　　**字　　数**：221千字
版　　次：2012年7月第1版　　**印　　次**：2012年7月第1次印刷
印　　数：1～　000
定　　价：　.00元

产品编号：041855-01

21世纪本科财经管理类专业实验与实践系列规划教材

编写委员会成员

序

PREFACE

目前，我国财经类院校在人才培养过程中比较注重专业知识和技能的传授与培养，而对跨专业的行业通识教育重视不足。本套教材是上海商学院在几年探索与实践基础上，逐步形成的经管类各专业通识性教育系列实践教材。

本套教材由长期从事财经类专业教学一线教师与企业专家共同编写。教材主要包括信息管理类、营运资金管理类、人力资源管理类、商贸应用扩展类和技能培训类五大模块的实验实训内容。通过本套教材学习，学生可以具备经管类跨专业的基本素养，为以后的职业发展打下扎实的实践基础。为了更好地训练学生自主学习能力，本套教材还配套编写了支持学生自主学习的网络实践学习指导。本套教材可用于财经类本科学校普适性实践教学。

胡巧多

2012 年 5 月

前言

FOREWORD

信息技术的高速发展给社会发展带来重大影响，也严重影响了人们的生产和生活。人们对信息的依赖越来越大，同样，人们对信息的安全也提出了更高的要求。

信息化给人们带来新的社会安全问题，尤其以网络环境为中心的信息系统的安全问题不同于传统意义的安全，它具有新的形势和特点。无论是在信息安全管理方面，还是在电子商务应用技术方面，人才是核心要素，需要不同领域、不同层次的多方面人才，特别是高素质复合型人才尤为重要。

本书为高校非计算机专业学生特别撰写，它结合了现场实验的软硬件环境，并充分考虑了学生的培养特点以及将来就业的客观社会需求，力求让学生通过实验实践，将理论知识与实际应用相结合。

真实、体验、直观是本书的特色。

本书共分 8 章，分别为操作系统篇、网络系统安全篇、病毒篇、应用安全篇、数据库篇、电子商务应用篇、电子商务环境搭建与营销支付篇和电子商务物流篇，每章前均有相关的理论知识的介绍。本课程建议学时为 32～36 学时，同时共附有 13 个实验，在实际教学过程中，可根据学生的具体情况和学时，做适当的删减，建议每章至少完成一个实验。

本书由张新谊任主编，蒋传进编写了第 6 章、第 7 章和第 8 章，蔡京玫编写了第 3 章，叶龙编写了第 5 章，其余由张新谊编写并统稿。

在本书的编写过程中，得到了上海庚商网络信息技术有限公司和南京奥派信息技术有限公司的大力支持，在此一并致谢。

由于编者水平所限，书中一定存有不足之处，敬请读者提出宝贵意见和建议。

编　者

2012 年 3 月于上海

目录

CONTENTS



第1章

操作系统篇

1.1 引言

操作系统是计算机中最基础、最重要的系统软件,各种应用程序要想运行,必须依赖于操作系统提供的系统软件,没有安全操作系统的支撑,安全保密性也就无从谈起。利用 Windows Server 2003 系统自身的安全工具,通过身份验证、账户管理、权限管理、日志管理等可以制定一套完善的计算机安全防护策略,维护 Windows 操作系统的基本安全。

1.2 操作系统概述

1.2.1 操作系统的功能

操作系统的主要功能,可以从以下三个方面来讨论:

(1) 管理计算机系统的硬件、软件、数据等各种资源,尽可能减少人工分配资源的工作以及人对机器的干预,发挥计算机的自动工作效率。

(2) 协调各种资源在使用过程中的关系,使得计算机的各种资源使用调度合理,高速设备与低速设备运行相互配合。

(3) 为用户提供使用计算机系统的环境,方便使用计算机系统的各部件或功能。操作系统通过自己的程序,将计算机系统的各种资源所提供的功能抽象出来,形成与之等价的操作系统的功能,并形象地表现出来,提供给用户,让其方便地使用计算机。

1.2.2 操作系统的分类

从用途的角度,操作系统可分为专用操作系统和通用操作系统两类。专用操作系统

是指用于控制和管理专项事物的操作系统，如现代手机中使用的操作系统，这类系统一般以嵌入硬件的方式出现，用于特定的用途。通用操作系统具有完善的功能，能够适应多种用途的需要。

从单机和网络的角度，操作系统可分为单机操作系统和网络操作系统。单机操作系统是针对单个计算机系统的环境设计的，它只有管理本机系统资源的功能。单用户操作系统是一种更为特殊的单机操作系统，它是针对一台机器、一个用户而设计的操作系统，它的基本特征是一次只能支持一个用户作业的运行，系统的所有资源由该用户独占，该用户对整个计算机系统有绝对的控制权。

从功能的角度，操作系统可分为批处理操作系统、分时操作系统、实时操作系统、网络操作系统、分布式操作系统。批处理操作系统、分时操作系统和实时操作系统的运行环境大多是单计算机系统，而网络操作系统和分布式操作系统的运行环境是多计算机系统。

1. 批处理操作系统

批处理操作系统的基本特征是"批量"，即将要交给计算机处理的若干个作业组织成队列成批地交给计算机自动地按作业队列顺序逐个处理。它可分为单道批处理操作系统和多道批处理操作系统。单道批处理操作系统一次只能调入一个处理作业在计算机内运行，其他作业放在辅助存储器上，它类似于单用户操作系统。计算机在运行处理作业时，时间主要消耗在两个方面：一方面是消耗在 CPU 执行程序上；另一方面是消耗在输入输出上。由于输入输出设备的速度相对于 CPU 执行程序的速度慢很多，导致计算机在输入输出时 CPU 处于空闲状态。为了提高 CPU 的使用效率，出现了多道批处理操作系统。它与单道批处理操作系统的区别是在计算机内存中可以有多个作业存在，调度程序根据事先确定的策略，选择一个作业将 CPU 资源分配给它运行处理，当处理的作业要进入输入输出操作时，就释放对 CPU 的占有，调度程序则从内存中等待处理的作业中选择一个交给 CPU 执行，这样，就提高了 CPU 的使用效率。

2. 分时操作系统

分时是指两个或两个以上的事件按时间划分轮流使用计算机系统的某一资源（主要是 CPU 资源）。在一个系统中如果多个用户分时使用一个计算机，那么这样的系统称为分时操作系统。分时的时间单位称为时间片，一个时间片一般是几十毫秒。在一个分时操作系统中，往往要连接几十个甚至上百个终端，每个用户在自己的终端上控制其作业的运行。通过操作系统的管理，将 CPU 轮流分配给各个用户使用。

3. 实时操作系统

实时操作系统要求实时处理并快速给出处理结果。实时操作系统一般是采用时间驱动的设计方法，系统能够及时对随时发生的事件做出响应并及时处理。实时操作系统分为实时控制操作系统和实时处理操作系统。实时控制操作系统常用于工业控制，以及飞行器、导弹发射等军事方面的自动控制。实时处理操作系统常用于预订飞机票、航班

查询，以及银行之间账务往来等。

4. 网络操作系统

随着计算机技术的迅速发展和网络技术的日益完善，不同地域的、具有独立处理能力的多个计算机系统通过通信设施互联，实现资源共享，组成计算机网络，成为一种更开放的工作环境，网络操作系统也应运而生。网络操作系统除了具有单机操作系统的所有功能以外，还具有网络资源的管理功能，支持网络应用程序运行。

5. 分布式操作系统

分布式操作系统是为分布式计算机系统配置的操作系统。分布式计算机系统与计算机网络一样，多台计算机系统通过通信网络互联，实现资源共享，但不同的是系统中的各个计算机没有主次之分，各计算机具有相对的自治性，用户访问共享资源时，不需要知道该共享资源位于哪台计算机上，如需要的话，系统中的多台计算机可以相互协作共同完成一个任务，即可以将一个任务分割成若干个子任务分散到多台计算机上同时并行执行。实际上，一种商用操作系统往往包括了批处理操作系统、分时操作系统、实时操作系统、网络操作系统、分布式操作系统等多方面的功能。不同的操作系统根据自身用途的定位和面向的用户，在各种功能的强弱上会有所区别。

1.3　Windows Server 2003 安全策略

随着信息化进程的加快，网络迅速发展，网络安全的重要性也渐渐凸现。网络安全涉及各个方面，而网络操作系统的安全设置很关键，Windows Server 2003 网络操作系统用户众多，是各种网络建设的首选，Windows Server 2003 网络操作系统沿袭了 Windows 的传统，在网络管理方面引入许多新的功能，提供了更高的硬件支持和更加强大的安全功能，如何用好 Windows Server 2003 的安全策略，怎样选择合理的设置，使网络安全配置得更好，对企业网、校园网、政务网等是至关重要的，要设置好 Windows Server 2003 网络操作系统的安全配置，必须了解 Windows Server 2003 网络操作系统的安全策略，分析 Windows Server 2003 网络操作系统的安全策略。

1.3.1　账户安全策略

账户安全策略包括密码策略、账户锁定策略和 Kerberos 策略三个方面，用户账户的保护主要是密码保护。通常采取提高密码的破解难度、启用账户锁定策略、限制用户登录等措施。密码策略用于域账户或本地用户账户。在 Windows Server 2003 系统中，可以通过账户策略设置中的“密码策略”来进行设置。通过提高密码的复杂性、增大密码的长度、提高更换频率等措施来提高密码的破解难度。该策略通过确保旧密码不能在某段时间内重复使用，使用户账户更安全。

要维持密码历史记录的有效性，则在通过启用密码最短使用期限安全策略，设置更改密码之后，不允许立即更改密码。可将密码的过期天数设置为 1～999 天；如果将天数

设置为0,则指定密码永不过期。使密码每隔30～90天过期一次是一种较好的安全选择。用这种方式,攻击者只能够在有限的时间内破解用户密码并访问网络资源。账户锁定策略用于域账户或本地用户账户,包含账户锁定时间、账户锁定阈值,以及复位账户锁定计数器。账户锁定是指在某些情况下为保护该账户的安全而将此账户进行锁定。使其在一定的时间内不能再次使用,从而挫败连续的猜解尝试。账户锁定时间确定锁定的账户在自动解锁前保持锁定状态的分钟数。有效范围为0～99 999分钟。如果将账户锁定时间设置为0,那么在管理员明确将其解锁前,该账户将被锁定。如果定义了账户锁定阈值,则账户锁定时间必须大于或等于重置时间,默认值为无。因为只有当指定了账户锁定阈值时,该策略设置才有意义。账户锁定阈值,该安全设置确定造成用户账户被锁定的登录失败尝试的次数。无法使用锁定的账户,除非管理员进行了重新设置或该账户的锁定时间已过期。登录尝试失败的范围可设置为0～999。如果将此值设为0,则将无法锁定账户。复位账户锁定计数器,该安全设置确定在登录尝试失败计数器被复位为0(即0次失败登录尝试)之前,尝试登录失败之后所需的分钟数。有效范围为1～99 999分钟。如果定义了账户锁定阈值,则该复位时间必须小于或等于账户锁定时间。Windows Server 2003系统在默认情况下,这种锁定策略并没有进行设定,对黑客的攻击没有任何限制。账户锁定策略设定的第一步就是指定账户锁定的阈值,即锁定前该账户无效登录的次数。一般设置账户锁定阈值为3次,如果3次登录全部失败,就会锁定该账户。Kerberos V5身份验证协议是用于确认用户或主机身份的身份验证机制,也是Windows Server 2003系统默认的身份验证服务。为防止“轮番攻击”,Kerberos V5在其协议定义中使用了时间戳。为使时间戳正常工作,客户端和域控制器的时钟应尽可能地保持同步。如果客户端时钟和域控制器时钟间的差值小于该策略中指定的最大时间差,那么在这两台计算机的会话中使用的任何时间戳都将被认为是可信的。

1.3.2 本地策略

本地策略包含审核策略、公钥策略、软件限制策略等。审核策略包含9个策略选项。系统审核机制可以对系统中的各类事件进行跟踪记录并写入日志文件,以供管理员进行分析、查找系统和应用程序故障,以及各类安全事件。对Windows Server 2003系统来说,为了不影响系统性能,默认的安全策略并不对安全事件进行审核。从“安全配置和分析”工具用SecEdit安全模板进行的分析结果可知,这些有红色标记的审核策略应该已经启用,这可用来发现来自外部和内部的黑客的入侵行为。对于关键的应用服务器和文件服务器来说,应同时启用剩下的安全策略。如果已经启用了“审核对象访问”策略,那么就要求必须使用NTFS文件系统。NTFS文件系统不仅提供对用户的访问控制,而且还可以对用户的访问操作进行审核。但这种审核功能,需要针对具体的对象来进行相应的配置。首先在被审核对象“安全”属性的“高级”属性中添加要审核的用户和组。在该对话框中选择好要审核的用户后,就可以设置对其进行审核的事件和结果。在所有的审核策略生效后,就可以通过检查系统的日志来发现黑客的蛛丝马迹。

在系统中启用安全审核策略后，管理员应经常查看安全日志的记录，否则就失去了及时补救和防御的时机了。除了安全日志外，管理员还要注意检查各种服务或应用的日志文件。在 Windows Server 2003 IIS 6.0 中，其日志功能默认已经启动，并且日志文件存放的路径默认在 System32/LogFiles 目录下，打开 IIS 日志文件，可以看到对 Web 服务器的 HTTP 请求，IIS 6.0 系统自带的日志功能从某种程度上可以成为入侵检测的得力帮手。使用 Syskey 保障密码信息的安全。保存在活动目录中的域账号密码信息是最为敏感的安全信息。系统密钥(System Key，Syskey)就是用来加密保存在域控制器的目录服务数据库中的账号密码信息的。Syskey 一共有三种工作模式。一是所有 Windows Server 2003 中默认采用的，计算机随机产生一个系统密钥，并将密钥加密后保存在本地。在这种模式中，可以像平时一样地登录本地计算机。二是系统密钥使用和模式一中的生成方式和存储方式相同，但是它使用一个由管理员指定的附加密码以提供更进一步的安全性。当重新启动计算机时，必须在启动的时候输入管理员指定的附加密码，这个密码不保存在本地。三是安全性最高的操作方法，计算机随机产生的系统密钥将被保存在一张软盘上，而不是本地计算机。如果没有软盘的物理访问权限，并在系统提示时插入该软盘，就无法引导系统。保护域控制器是网络安全策略中的重要一步。

1.3.3 IPSec 策略

IPSec 策略是安全联网的长期方向。它通过端到端的安全性来提供主动的保护，为防止专用网与 Internet 的攻击提供了主要防线，在源 IP 地址和目标 IP 地址之间建立信任和安全性。IPSec 策略由常规 IPSec 策略设置和 IPSec 策略规则组成。由于在 IP 协议设计之初并没过多考虑安全问题，因此早期的网络中经常发生遭受攻击或机密数据被窃取等问题。为了增强网络的安全性，IP 安全(IPSec)协议应运而生。

为了增强网络通信安全或对客户机器的管理，网络管理员可以通过在 Windows 系统中定义 IPSec 安全策略来实现。一个 IPSec 安全策略由 IP 筛选器和筛选器操作两部分构成，其中 IP 筛选器决定哪些报文应当引起 IPSec 安全策略的关注，筛选器操作是指“允许”还是“拒绝”报文的通过。要新建一个 IPSec 安全策略，一般需要新建 IP 筛选器和筛选器操作。

基于 IP 的网络通信技术没有内建的安全机制。随着互联网的发展，安全问题逐渐暴露出来。现在经过各个方面的努力，标准的安全架构也已经基本形成。那就是 IPSec 机制，并且它将作为下一代 IP 网络标准 IPv6 的重要组成。IPSec 机制在新一代的操作系统中已经得到了很好的支持。在 Windows Server 2003 系统中，其服务器产品和客户端产品都提供了对 IPSec 的支持。从而增强了安全性、可伸缩性以及可用性，同时使部署和管理更加方便。在 Windows Server 2003 系统的安全策略相关的管理工具集(如本地安全策略、域安全策略、组策略等)中，都集成了相关的管理工具。用户可以根据情况来添加、修改和删除相应的 IP 安全策略。其中 Windows Server 2003 系统自带的策略如下。

(1) 采用 IPSec 加密数据通信的方法适用于企业网应用，通过部署组策略可以强制网络中的所有计算机使用 IPSec 加密通信。当然这种严格地限制会带来一些不便，不过对于系统安全来说是值得的。

(2) IPSec 还可以应用于 VPN 技术中，在这里可以对 IP 隧道中的数据流进行加密。对于不方便大范围实施 IPSec 的环境，可以考虑采用 VPN 技术。VPN 技术是目前实现端对端安全通信的最佳解决方案。

1.3.4 配置连接请求策略

对于企业网络，需要为一些远程拨号的用户提供拨号接入服务。远程拨号访问实际上是通过低速的拨号连接来将远程计算机接入到企业内部的局域网中。由于这个连接无法隐藏，因此常常成为黑客入侵内部网络的最佳入口。对于基于 Windows Server 2003 的远程访问服务器来说，默认情况下将允许具有拨入权限的所有用户建立连接。因此，安全防范的第一步就是合理地、严格地设置用户账户的拨入权限，严格限制拨入权限的分配范围，只要不是必要的就不给予此权限。对于网络中的一些特殊用户和固定的分支机构的用户来说，可通过回拨技术来提高网络安全性，这样就需要开通来电显示业务。

在 Windows Server 2003 网络中，如果活动目录工作在 Native-mode 下，这时就可以通过存储在访问服务器上或 Internet 验证服务器上的远程访问策略来管理。针对各种应用场景的不同，可以设置多种不同的策略。

1.3.5 防火墙策略

防火墙是网络安全的屏障。ISA Server 防火墙是建立在 Windows 操作系统上的一种可扩展的企业级防火墙，支持两个层级的策略：阵列级策略和企业级策略。

阵列级策略包括站点和内容规则、协议规则、IP 数据包筛选器、Web 发布规则和服务器发布规则。修改阵列配置时，该阵列内所有的 ISA Server 计算机也都会被修改，包括所有的访问策略和缓存策略。

企业级策略进一步体现了集中式管理，它允许设置一项或多项应用于企业网阵列的企业策略。企业级策略包括站点和内容规则，以及协议规则。企业级策略可用于任何阵列，而且可通过阵列自己的策略进行扩充。Windows Server 2003 支持 ISA Server 2000，但要安装补丁，为 ISA Server 升级。

1.3.6 组策略

Windows Server 2003 组策略和安全模板组策略用于从一个单独的点对多个 Microsoft Active Directory 目录服务用户和计算机对象进行配置。在默认情况下，策略不仅影响应用该策略的容器中的对象，还影响子容器中的对象。组策略包含了“计算机配置”→“Windows 设置”→“安全设置”下的安全设置。应用组策略可自动更新，但为了立即启动更新过程，可在命令提示符下使用 GPUpdate 命令，启用“安全配置和分析”。

在 Windows Server 2003 网络中，还有一种非常有效的防范黑客入侵和管理疏忽的辅助手段，这就是利用“受限制的组”安全策略。该策略可保证组成员的组成固定。首先，在域安全策略的管理工具中添加要限制的组，在“组”对话框中输入或查找要添加的组。一般要对管理员组等特权组的成员加以限制。其次，要配置这个受限制的组的成员。在这里选择受限制的组的“安全性”选项。然后，就可以管理这个组的成员组成，可以添加或删除成员，当安全策略生效后，可防止黑客将后门账户添加到该组中。

1.3.7　软件限制策略

软件限制策略可以标识软件并控制它在本地计算机、组织单位、域或站点中的运行能力。可以帮助计算机防范电子邮件病毒。使用软件限制策略，先要进行创建，为软件限制策略创建单独的组策略对象。如果应用策略设置后遇到了问题，以安全模式重新启动计算机操作系统。

1.4　系统漏洞

系统漏洞又被称为“安全缺陷”或者“系统 BUG”，同时也成为黑客为了达到他们的攻击目的而寻找的一个攻击入口。据统计，一台未打补丁的系统，接入互联网后，不到 2 分钟就会受到各种漏洞所攻击，并导致计算机中毒或崩溃。

从各种信息资源中，人们或许已经对网络“漏洞”这个概念有了一些感性的了解。其实，“漏洞”并非一个物理上的概念。漏洞是指程序在设计、实现或运行操作上的错误，而被黑客用来获取信息、取得用户权限、取得系统管理员权限或破坏系统。但是关于网络漏洞，目前还没有一个准确统一的定义。一个较为通俗的网络漏洞的描述性定义是：存在于计算机网络系统中的、可能对系统中的组成和数据造成损害的一切因素。当对系统的各种操作与系统的安全策略发生冲突时，就产生了安全漏洞。也可以解释为：计算机系统是由若干描述实体配置的当前状态所组成，可分为授权状态和非授权状态、易受攻击状态和不易受攻击状态，漏洞就是状态转变过程中能导致系统受损的、易受攻击状态的特征。以上说法，都是从不同的专业角度对网络漏洞进行的描述，但并没有给出一个全面的、准确的定义。总之，在计算机安全领域，网络漏洞就是指网络的脆弱性问题。

1.4.1　漏洞扫描系统工作原理

漏洞扫描器是一种自动检测远程或本地主机安全性弱点的程序。通过使用漏洞扫描器，系统管理员能够发现所维护的 Web 服务器的各种 TCP 端口的分配、提供的服务、Web 服务软件版本和这些服务及软件呈现在 Internet 上的安全漏洞。从而在计算机网络系统安全保卫战中做到“有的放矢”，及时修补漏洞，构筑坚固的安全长城。漏洞扫描器属于主动的探测行为，即向对方主机发送包含漏洞探测码的数据包，然后等待对方的反应，根据对方的反应与漏洞特征码比较来判断漏洞是否存在。实现漏洞扫描器本质上

只需要实现三个部分：发送数据包构件、接收数据包构件和漏洞特征码数据库。系统漏洞是一个全世界都在关注的话题。因为系统漏洞给计算机的安全带来了很大的隐患，但是系统漏洞的产生却很难避免。这是因为随着软件复杂度的提高，给管理和检测都带来了很大难题。有的漏洞的产生是由于程序员的粗心大意或者考虑不周引起的，有的系统漏洞却是由于软件模块之间的配合衔接引起的。这些漏洞都令人防不胜防。所以至今，对系统漏洞仍然没有有效的避免方法，世界上每天都会发现大量的系统漏洞。既然系统漏洞难以避免，那么如何扫描系统漏洞便成了当务之急。现今发展出来的系统漏洞扫描的办法主要有两种：一是根据系统漏洞的情况对系统进行攻击，以此来判定系统漏洞的存在；二是根据系统中相关软件的版本号来判定系统中存在的漏洞。系统漏洞扫描框架如图 1.1 所示。

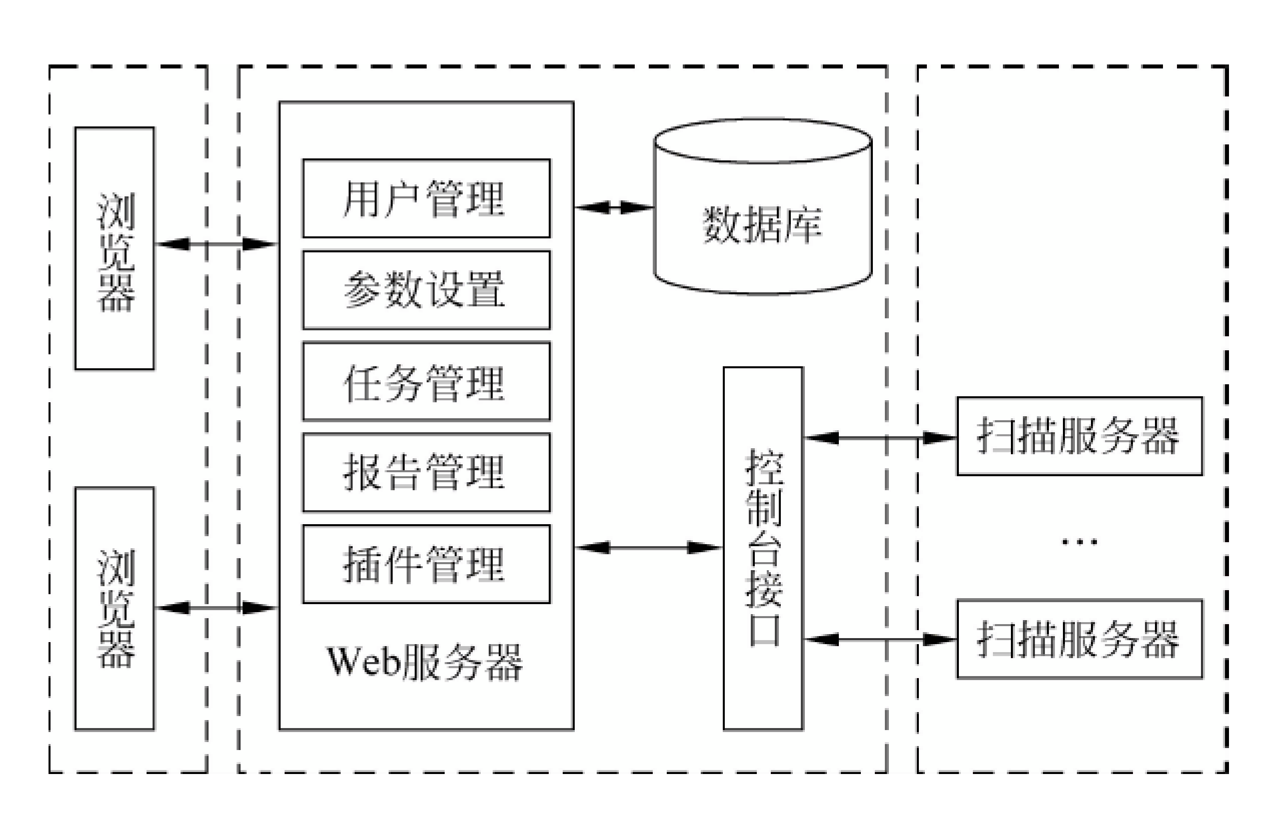


图 1.1 系统漏洞扫描框架

扫描系统有三种最基本的功能：发现一个主机和网络的能力；一旦发现一台主机，即有发现什么服务正运行在这台主机上的能力；通过测试这些服务，即有发现这些漏洞的能力。扫描器对 Internet 安全很重要，因为它能揭示一个网络的弱点。在任何一个现有的平台上都有几百个熟知的安全弱点。在大多数情况下，这些弱点都是唯一的，仅影响一个网络服务。人工测试单台主机的弱点是一项极烦琐的工作，而扫描程序能轻易地解决这些问题。扫描程序开发者利用可得到的常用攻击方法并把它们集成到整个扫描中，这样使用者就可以通过分析输出的结果发现系统的漏洞。扫描器一般采用模拟攻击的形式对网络上目标计算机可能存在的已知安全漏洞进行逐项检查，目标可以是工作站、服务器、交换机、数据库应用等各种对象，然后根据扫描结果向系统管理员提供周密可靠的安全性分析报告，为提高网络安全整体水平产生重要依据。在网络安全体系中，安全扫描工具具有花费低、效果好、见效快、与网络的运行相独立、安装运行简单等优点。可以大大减少网络管理员操作的复杂性，有利于网络的安全和稳定。

1.4.2 漏洞扫描技术的实现

用手工进行扫描时需要熟悉相关的网络命令，并且能够对命令执行后的输出进行分

析。下面介绍端口扫描分析涉及的几个常用网络命令。

(1) Host 命令：这是一个 UNIX 命令，Host 命令的危险性相当大，这个命令的执行结果所得到的信息十分多。包括操作系统、机器和网络的很多数据。任何人都能通过在命令行中输入一个命令，就能收集到一个域中的所有计算机的重要信息，而且只需要几秒钟的时间。

(2) Showmount 命令：该命令可以发现远程主机的一些非常有用的信息。通过加入-e 命令选项，Showmount 命令可以提供指定目标上所有对外目录的清单。

(3) Rusers 和 Finger 都是 UNIX 命令。通过这两个命令，能收集到目标计算机上的有关用户的消息。这个命令能显示用户的状态，该命令是建立在客户/服务模型之上的。用户通过客户端软件向服务器请求信息，然后解释这些信息，提供给用户。在服务器上一般运行一个称为 Fingerd 的程序，根据服务器的配置，能向客户提供某些信息。如果考虑到保护这些个人信息的话，有可能许多服务器不提供这个服务，或者只提供一些无关的信息。

(4) Ping 命令经常用来对 TCP/IP 网络进行诊断。通过目标计算机发送一个数据包，让它将这个数据包返送回来。如果返回的数据包和发送的数据包一致，那就说明 Ping 命令成功了。通过这样对返回的数据进行分析，就能判断计算机是否开着，或者这个数据包从发送到返回需要多少时间。

利用上述有用的网络命令，可收集到许多有用的信息。例如，一个域中的名字服务器的地址，一台计算机上的用户名，一台服务器上正在运行什么服务，这个服务是哪个软件提供的，计算机上运行的是什么操作系统。如果知道目标计算机上运行的操作系统和服务应用程序后，就能利用已经发现的漏洞来进行攻击。如果目标计算机的网络管理员没有对这些漏洞及时修补的话，入侵者就能轻而易举地闯入该系统，获得管理员权限，并留下后门。如果入侵者得到目标计算机上的用户名后，能使用口令破解软件。多次试图登录目标计算机，经过尝试后，就有可能进入目标计算机。得到了用户名，就等于得到了一半的进入权限，剩下的只是使用软件进行攻击而已。

1.4.3 TCP/IP 相关问题

典型的扫描器是 TCP 端口扫描器。这种程序可以选择 TCP/IP 端口和服务，并记录目标主机的回答。通过这种方法，可以搜集到关于目标主机的有用信息。而 UNIX 平台下的扫描器一般用于观察某一服务是否正在一台远程机器上正常工作。它们并不是通常意义上的 TCP/IP 扫描器，但也可用于收集目标主机的信息。下面介绍端口扫描技术涉及的一些 TCP/IP 方面的关键内容。

(1) 连接端及标志：IP 地址和端口被称为套接字，它代表 TCP 连接的一个连接端。为了获得 TCP 服务，必须在发送机的一个端口上和接收机的一个端口上建立连接。TCP 连接用两个连接端来区别，也就是连接端 1 和连接端 2。连接端互相发送数据包。一个 TCP 数据包包括一个 TCP 头，后面是选项和数据。一个 TCP 头包含 6 个标志位。

它们的意义分别如下。

SYN：用来建立连接，让连接双方同步序列号。如果 SYN=1 而 ACK=0，则表示该数据包为连接请求；如果 SYN=1 而 ACK=1 则表示接受连接。

FIN：表示发送端已没有数据要求传输了，希望释放连接。

RST：用来复位一个连接。RST 标志位置位的数据包称为复位包。一般情况下，如果 TCP 收到的一个分段明显不是属于该主机上的任何一个连接，则向远端发送一个复位包。

URG：为紧急数据标志位。如果 URG=1，表示本数据包中包含紧急数据。此时紧急数据指针有效。

ACK：为确认标志位。如果 ACK=1，表示包中的确认号是有效的。否则，包中的确认号无效。

PSH：如果置位，接收端应尽快把数据传送给应用层。

(2) TCP 连接的建立：TCP 是一个面向连接的可靠传输协议。面向连接表示两个应用端在利用 TCP 传送数据前必须先建立 TCP 连接。TCP 的可靠性通过校验和定时器、数据序号和应答来提供。通过给每个发送的字节分配一个序号，接收端接收到数据后发送应答，TCP 协议保证了数据的可靠传输。数据序号用来保证数据的顺序，剔除重复的数据。在一个 TCP 会话中，有两个数据流(每个连接端从另外一端接收数据，同时向对方发送数据)，因此在建立连接时，必须要为每一个数据流分配 ISN(初始序号)。大部分 TCP/IP 实现遵循以下原则：

① 当一个 SYN 或者 FIN 数据包到达一个关闭的端口时，TCP 丢弃数据包同时发送一个 RST 数据包；

② 当一个 RST 数据包到达一个监听端口时，RST 被丢弃；

③ 当一个 RST 数据包到达一个关闭的端口时，RST 被丢弃；

④ 当一个包含 ACK 的数据包到达一个监听端口时，数据包被丢弃，同时发送一个 RST 数据包；

⑤ 当一个 SYN 位关闭的数据包到达一个监听端口时，数据包被丢弃；

⑥ 当一个 SYN 数据包到达一个监听端口时，正常的三阶段握手继续，回答一个 SYN、ACK 数据包；

⑦ 当一个 FIN 数据包到达一个监听端口时，数据包被丢弃。“FIN 行为”(关闭的端口返回 RST，监听端口丢弃包)，在 URG、PSH 标志位置位时同样要发生。所有的 URG、PSH 和 FIN，或者没有任何标志的 TCP 数据包都会引起“FIN 行为”。

1.4.4 全 TCP 连接扫描和 TCP SYN 扫描技术

1. 全 TCP 连接扫描

这是最基本的 TCP 扫描，实现方法最简单。直接连接到目标端口并完成一个完整的三次握手过程(SYN、SYN/ACK 和 ACK)。操作系统提供的 Connect()系统调用，用

来与每一个感兴趣的目标计算机的端口进行连接。如果端口处于监听状态，那么Connect()就能成功；否则，这个端口是不能用的，即没有提供服务。这个技术的一个最大优点是不需要任何权限，系统中的任何用户都可以使用这个调用。另一个好处就是速度，如果对每个目标端口以线性的方式，使用单独的Connect()调用，那么将会花费相当长的时间。可以通过同时打开多个套接字，从而加速扫描。使用非阻塞I/O允许设置一个低的时间用尽周期，同时观察多个套接字。这种扫描方法的缺点是很容易被目标系统检测到，并且被过滤掉。目标计算机的日志文件会显示大量密集的连接和连接出错的消息记录，并且能很快地使它关闭。Courtney、Gabriel和TCP Wrapper监测程序通常用来进行监测。另外TCP Wrapper可以对连接请求进行控制，所以它可以用来阻止来自不明主机的全TCP连接扫描。

2. TCP SYN 扫描

在这种技术中，扫描主机向目标主机的选择端口发送SYN数据段。如果应答是RST，那么说明端口是关闭的。按照设定监听其他端口，如果应答中包含SYN和ACK，说明目标端口处于监听状态。由于在SYN扫描时，全连接尚未建立，所以这种技术通常被称为半打开扫描。SYN扫描的优点在于即使日志中对扫描有所记录，但是尝试进行连接的记录也要比全扫描少得多；缺点是在大部分操作系统下，发送主机需要构造适用于这种扫描的IP包。并且在通常情况下必须要有超级用户权限才能建立自己的SYN数据包。

3. 利用ICMP协议的扫描技术

Ping就是利用ICMP协议实现的。在扫描技术中可以利用ICMP协议最基本的用途：报错。根据网络协议，如果协议出现了错误，那么接收端将产生一个ICMP的错误报文。这些错误报文并不是主动发送的，而是由于错误，根据协议自动产生。当IP数据报出现Checksum和版本错误时，目标主机将抛弃这个数据报；如果是Checksum出现错误，那么路由器就会直接丢弃这个数据报。可以利用下面这些特性：

（1）向目标主机发送一个只有IP头的IP数据包，目标将返回Destination Unreachable的ICMP错误报文。

（2）向目标主机发送一个坏IP数据报，如不正确IP头长度。目标主机将返回Parameter Problem的ICMP错误报文。

（3）当数据包分片但却没有给接收端足够的分片。接收端分片组装超时会发送分片组装超时的ICMP数据报。向目标主机发送一个IP数据报，但是协议项是错误的，如协议项不可用，那么目标将返回Destination Unreachable的ICMP报文。但是如果是在目标主机前有一个防火墙或者一个其他的过滤装置，可能过滤掉提出的要求，从而接收不到任何回应。可以使用一个非常大的协议数字来作为IP头部的协议内容，而且这个协议数字还没有被使用。主机一定会返回Unreachable。如果没有Unreachable的ICMP数据报返回错误提示，那么就说明被防火墙或者其他设备过滤了。可以用这个办法来探测是否有防火墙或者其他过滤设备存在。利用IP的协议项来探测主机正在使用哪些协

议,可以把 IP 头的协议项改变。因为是 8 位的,有 256 种可能。通过目标返回的 ICMP 错误报文,来判断哪些协议在使用。如果返回 Destination Unreachable,那么主机是没有使用这个协议的。相反,如果什么都没有返回的话,主机可能使用这个协议,但是也可能是防火墙等过滤掉了。NMAP 的 IP Protocol Scan 也就是利用这个原理。利用 IP 分片造成组装超时 ICMP 错误消息,同样可达到探测目的。当主机接收到丢失分片的数据报,并且在一定时间内没有接收到丢失的数据报,就会丢弃整个包。并且发送 ICMP 分片组装超时错误给原发送端。可利用这个特性制造分片的数据包,然后等待 ICMP 组装超时错误消息,可对 UDP 分片,也可对 TCP 甚至 ICMP 数据包进行分片,只要不让目标主机获得完整的数据包就行了。当然,对于 UDP 这种非连接的不可靠协议来说,如果没有接收到超时错误的 ICMP 返回报文,也有可能是由于线路或者其他问题在传输过程中丢失了。

1.4.5 TCP 扫描与间接扫描

1. TCP FIN 扫描

TCP FIN 扫描对某端口发送一个 TCP FIN 数据报给远端主机,如果主机没有任何反馈,那么这个主机是存在的,而且正在监听这个端口;如果主机反馈一个 TCP RST 回来,那么说明该主机是存在的,但是没有监听这个端口。由于这种技术不包含标准的 TCP 三次握手协议的任何部分,所以无法被记录下来,从而比 SYN 扫描隐蔽得多。另外,FIN 数据包能够通过只监测 SYN 包的包过滤器。这种扫描方法的思想是关闭的端口会用适当的 RST 来回复 FIN 数据包。另一方面,打开的端口会忽略对 FIN 数据包的回复。这种方法和系统实现有一定的关系。有的系统不管端口是否打开,都回复 RST,此时这种扫描方法就不适用了。这种扫描技术使用 FIN 数据包来监听端口。当一个 FIN 数据包到达一个关闭的端口时,数据包会被丢掉,并且会返回一个 RST 数据包。否则,当一个 FIN 数据包到达一个打开的端口时,数据包只是简单的丢掉(不返回 RST)。这种技术通常适用于 UNIX 目标主机。跟 SYN 扫描类似,FIN 扫描也需要自己构造 IP 包。

2. 间接扫描

间接扫描的思想是利用第三方的 IP(欺骗主机)来隐藏真正扫描者的 IP。由于扫描主机会对欺骗主机发送回应信息,所以必须监控欺骗主机的 IP 行为,从而获得原始扫描的结果。假定参与扫描过程的主机为扫描机、隐藏机、目标机。扫描机和目标机的角色非常明显。隐藏机是一个非常特殊的角色。在扫描机扫描目标机时,它不能发送除了与扫描有关包以外的任何数据包。

1.4.6 认证扫描和 FTP 返回攻击的利用

1. 认证扫描

认证扫描能够获取监听端口进程的特征和行为。利用认证协议的扫描器能够获取

运行在某个端口上进程的用户名 Userid。认证扫描尝试与一个 TCP 端口建立连接，如果连接成功，扫描器发送认证请求到目的主机的 TCP 113 端口。认证扫描同时也被称为反向认证扫描。因为最初的 RFC 建议了一种帮助服务器认证客户端的协议，所以在实际的实现中也考虑了反向应用(即客户端认证服务器)。

2. FTP 返回攻击

FTP 协议支持代理 FTP 连接选项。这个选项允许一个客户端同时跟两个 FTP 服务器建立连接，然后在服务器之间直接传输数据。然而，在大部分实践中，实际上能使 FTP 服务器发送文件到 Internet 任何地方，许多攻击正是利用了这个缺陷，最近的许多扫描器利用这个弱点实现 FTP 代理扫描。FTP 端口扫描主要使用 FTP 代理服务器来扫描 TCP 端口。这种方法的优点是难以跟踪，能穿过防火墙；主要缺点是速度很慢，并且有的 FTP 服务器能够发现这些扫描代码，从而关闭其代理功能。

1.4.7　其他扫描方法

1. Ping 扫描

如果需要扫描一个主机上甚至整个子网上的成千上万个端口。首先判断一个主机是否开机就非常重要了，这就是 Ping 扫描器的目的。主要有两种方法用来实现 Ping 扫描：

① 真实扫描，例如，发送 ICMP 请求包给目标 IP 地址，有相应的返回就表示主机开机。

② TCP Ping，例如，发送特殊的 TCP 包给通常都打开且没有过滤的端口(如 80 端口)，对没有超级用户权限的扫描者，使用标准的 Connect 来实现。否则，ACK 数据包发送给每一个需要探测的主机 IP，每一个返回的 RST 表明相应主机开机。另外，一种类似于 SYN 扫描端口 80 也被经常使用。

2. IP 段扫描

此方法只是其他技术的变化，它不直接发送 TCP 探测数据包，而是将数据包分成两个较小的 IP 段。这样就将一个 TCP 头分成好几个数据包，从而过滤器就很难探测到。

3. TCP 反向 Ident 扫描

Ident 协议允许看到通过 TCP 连接的任何进程的拥有者的用户名，即使这个连接不是由这个进程开始的。因此，连接到 HTTP 端口，然后用 Ident 来发现服务器是否正在以超级用户权限运行。这种方法只能在和目标端口建立了一个完整的 TCP 连接后才能看到。

1.4.8　漏洞扫描

漏洞扫描是对重要计算机信息系统进行检查，发现其中可能被黑客利用的漏洞。漏洞扫描的结果是对系统安全性能的一个评估，它指出了哪些攻击是可能的，因此，漏洞扫

描成为安全方案的一个重要组成部分。目前，漏洞扫描，从底层技术来划分，可分为基于网络的漏洞扫描和基于主机的漏洞扫描两种类型。

1. 基于网络的漏洞扫描

基于网络的漏洞扫描器是通过网络来扫描远程计算机中的漏洞。例如，利用低版本的漏洞，攻击者能够获取权限侵入系统，或者攻击者能够在远程计算机中执行恶意代码。使用基于网络的漏洞扫描工具，能够监测到这些低版本的是否在运行。一般来说，基于网络的漏洞扫描工具可以看做一种漏洞信息收集工具，它根据不同漏洞的特性，构造网络数据包，发给网络中的一个或多个目标服务器，以判断某个特定的漏洞是否存在。基于网络的漏洞扫描器，一般由以下几个方面组成。

(1) 漏洞数据库模块：漏洞数据库包含了各种操作系统的各种漏洞信息，以及如何检测漏洞的指令。

(2) 用户配置控制台模块：用户配置控制台与安全管理员进行交互，用来设置要扫描的目标系统，以及扫描哪些漏洞。

(3) 扫描引擎模块：扫描引擎是扫描器的主要部件。根据用户配置控制台部分的相关设置，扫描引擎组装好相应的数据包，发送到目标系统，将接收到的目标系统的应答数据包，与漏洞数据库中的漏洞特征进行比较，来判断所选择的漏洞是否存在。

(4) 当前活动的扫描知识库模块：通过查看内存中的配置信息，该模块监控当前活动的扫描，将要扫描的漏洞的相关信息提供给扫描引擎。

(5) 结果存储器和报告生成工具：报告生成工具，利用当前活动扫描知识库中存储的扫描结果，生成扫描报告。

基于网络的漏洞扫描器的价格相对来说比较便宜。漏洞扫描器在操作过程中，不需要涉及目标系统的管理员，在检测过程中，不需要在目标系统上安装任何软件，维护简便。当企业的网络发生了变化时，只需要某个结点就能够扫描网络中的全部目标系统，基于网络的漏洞扫描器不需要进行调整。

2. 基于主机的漏洞扫描

基于主机的漏洞扫描器与基于网络的漏洞扫描器的原理类似，但是，两者的体系结构不一样。基于主机的漏洞扫描器通常目标系统上安装了一个代理或者服务，以便能够访问所有的文件与进程，这也使得基于主机的漏洞扫描器能够扫描更多的漏洞。基于主机的漏洞扫描具有如下优点。

(1) 扫描的漏洞数量多。由于通常在目标系统上安装了一个代理或者服务，以便能够访问所有的文件与进程，这也使得基于主机的漏洞扫描器能够扫描更多的漏洞。

(2) 集中化管理。基于主机的漏洞扫描器通常都有个集中的服务器作为扫描服务器。所有扫描的指令，均从服务器进行控制，这一点与基于网络的扫描器类似。服务器从下载到最新的代理程序后，再分发给各个代理。这种集中化管理模式，使得基于主机的漏洞扫描器的部署上，能够快速实现。

(3) 网络流量负载小。由于管理器与代理之间只有通信的数据包，漏洞扫描部分都

有代理单独完成，这就大大减少了网络的流量负载。当扫描结束后，代理再次与管理器进行通信，将扫描结果传送给管理器。

1.5　公钥体系原理

用户 A 有一对密钥，分为公钥和私钥，这对密钥是唯一的，是通过对一个巨大的素数进行因数分解所得到的，用公钥加密的信息，只能使用与它配对的私钥来解密，反之亦然，用私钥加密过的信息也只能用公钥来解密，这样，A 从认证体系生成一对密钥后，把它的私钥保存好，把公钥公开出去，当一个用户 B 要与 A 通信，又想确保数据安全时，就可以使用 A 的公钥来加密信息，再把密文传给 A，因此，这个世界上只有 A 手中的私钥才能对这个密文进行解密，这样就确保了信息的安全。

实验 1　Windows Server 2003 安全策略配置

一、实验目的

通过实验，了解 Windows Server 2003 的安全策略，组策略、强制使用安全的密码策略，并掌握远程访问的使用。

二、实验原理

Windows Server 2003 作为 Microsoft 最新推出的服务器操作系统，不仅继承了 Windows 2000/XP 的易用性和稳定性，而且还提供了更高的硬件支持和更加强大的安全功能，无疑是中小型网络应用服务器的首选。

提高密码的破解难度主要是通过采用提高密码复杂性、增大密码长度、提高更换频率等措施来实现，但这常常是用户很难做到的，对于企业网络中的一些安全敏感用户就必须采取一些相关的措施，以强制改变不安全的密码使用习惯。

在 Windows Server 2003 系统中可以通过一系列的安全设置，并同时制定相应的安全策略来实现。在 Windows Server 2003 系统中，可以通过在安全策略中的“密码策略”来进行设置。Window Server 2003 系统的安全策略可以根据网络的情况，针对不同的场合和范围进行有针对性的设定。例如，可以针对本地计算机、域及相应的组织单元来进行设定，这将取决于该策略要影响的范围。

本实验就针对 Windows Server 2003 在企业网络应用中系统账户和系统监控方面的安全策略的制定进行尝试验证，从而体会安全设置对于 Windows Server 2003 系统稳定运行的重要性，通过实验，深刻认识系统安全的隐蔽性和重要性。

三、实验内容

1. 实验环境

（1）PC 一台，用于客户端测试。

（2）服务器一台，用于设置 Windows 安全策略。

实验拓扑图和配置信息分别如图 1.2 和表 1.1 所示。

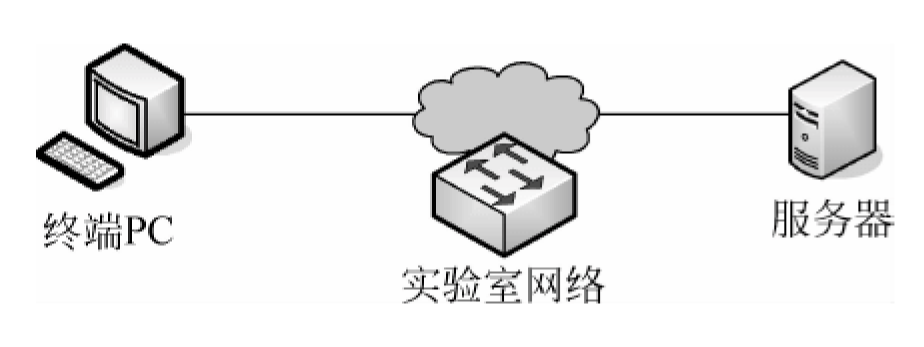


图 1.2 实验拓扑图

表 1.1 演示实验设备配置参考信息表

设备名称	IP 地址
示例实验终端 PC	192.168.1.100
示例实验 Windows Server 2003 服务器	192.168.1.251

2. 实验角色

本实验为单人验证实验，用于体验 Windows Server 2003 的组策略设置。可以通过管理员账户登录服务器设置组策略和用于策略，再用新增用户账户来验证实验。

3. 实验步骤

1）服务端配置

（1）启动远程连接。在终端 PC 中，执行“开始”→“运行”命令，打开“运行”对话框，在“打开”文本框中输入“mstsc”命令。

（2）连接远程服务器：打开“远程桌面连接”后，在“计算机”文本框中输入服务器的 IP 地址“192.168.1.251”。

（3）输入管理员用户名和密码登录服务器。在服务器上执行“开始”→“运行”命令，在“打开”文本框中输入“gpedit.msc”命令，打开“组策略编辑器”窗口，如图 1.3 所示。

（4）在“组策略编辑器”窗口中展开“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”。

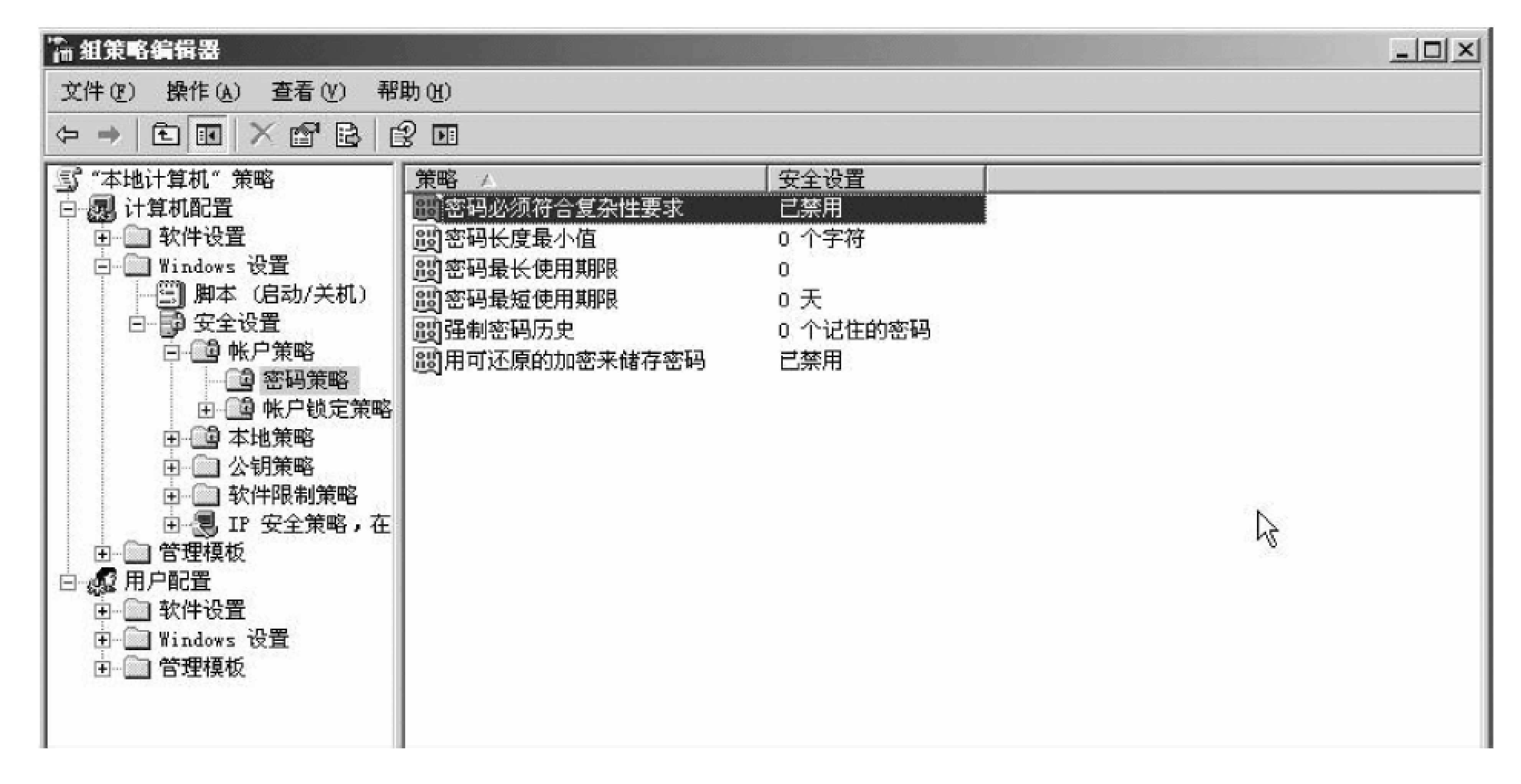


图 1.3 “组策略编辑器”窗口

（5）单击“密码必须符合复杂性要求”，设置密码复杂属性为“已启用”，如图 1.4 所示。



图 1.4　启用密码复杂性

(6) 在左导航栏选择“账户锁定策略”选项，在右边单击“账户锁定阈值”，如图 1.5 所示。

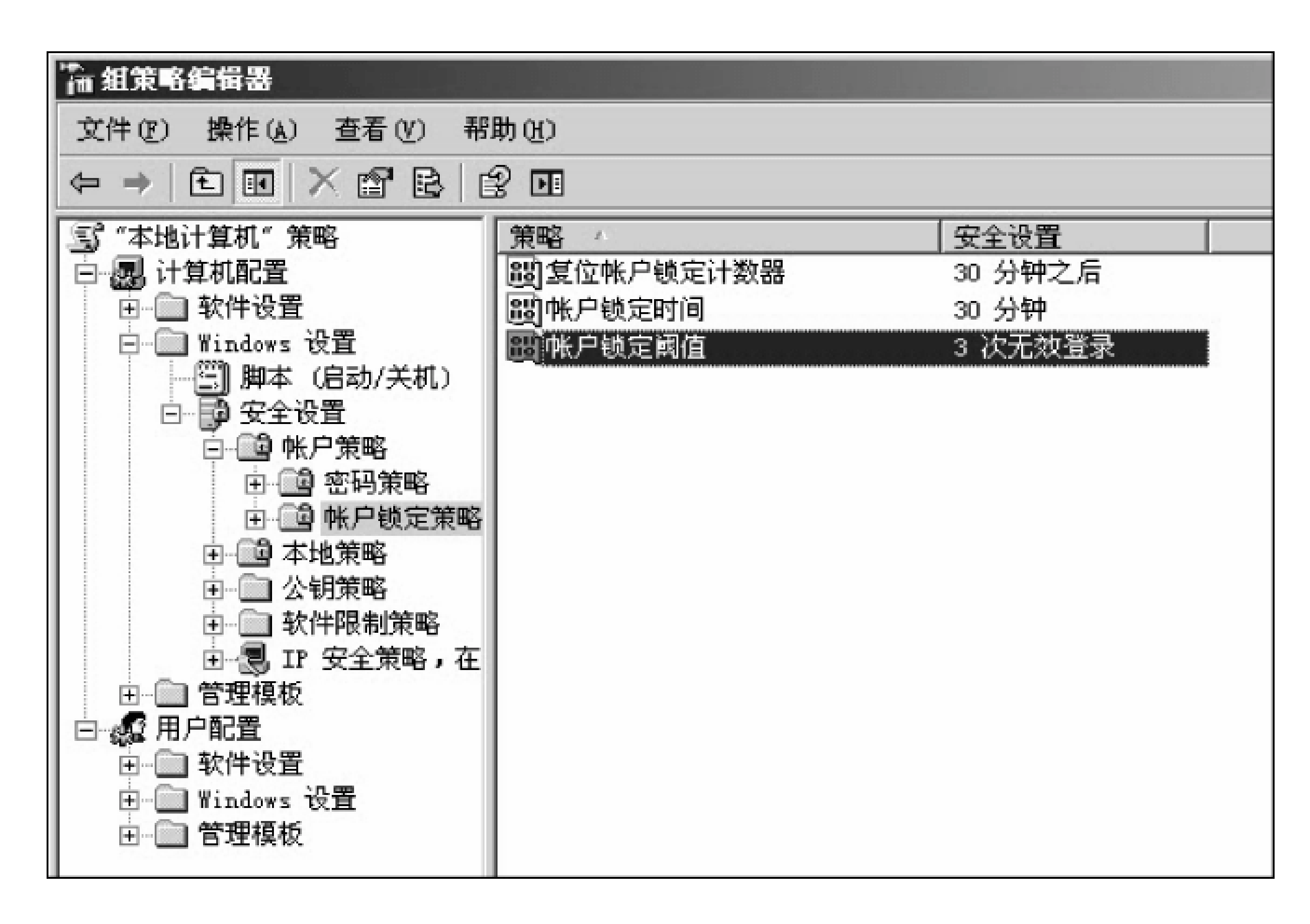


图 1.5　账户锁定阈值

(7) 在“本地安全设置”选项卡中，设置“3”次无效登录就锁定，如图 1.6 所示。



图 1.6　本地安全设置

(8) 在桌面上右击“我的电脑”,在弹出的快捷菜单中选择“管理”选项,打开“计算机管理”窗口。

(9) 在左导航栏展开“本地用户和组”→“用户”,在右侧空白处右击,在弹出的快捷菜单中选择“新用户”选项,如图 1.7 所示。



图 1.7 添加新用户

(10) 新用户名设为“talent”,密码设为“123”,会出现什么现象?

(11) 设置一个较长且复杂的密码,如“Shang_Hai_12345”。(注意:密码有大小写敏感,请重视。)

(12) 在新创建的用户上右击选择“属性”选项,在打开的“talent 属性”对话框中选择“隶属于”选项卡,然后把新用户添加到 Remote Desktop Users 组,如图 1.8 所示。(注意:把用户添加到此组是为了可以让客户端远程连接服务器)



图 1.8 新用户添加到 Remote Desktop Users 组

2) 客户端测试

(1) 在终端 PC 中,执行“开始”→“运行”命令,打开“运行”对话框,在“打开”文本框中输入“mstsc”命令。

(2) 打开“远程桌面连接”后,在“计算机”文本框中输入服务器的 IP 地址“192.168.1.251”。

（3）输入用户名“talent”和密码“Shang_Hai_12345”，然后单击“连接”按钮，如图1.9所示。

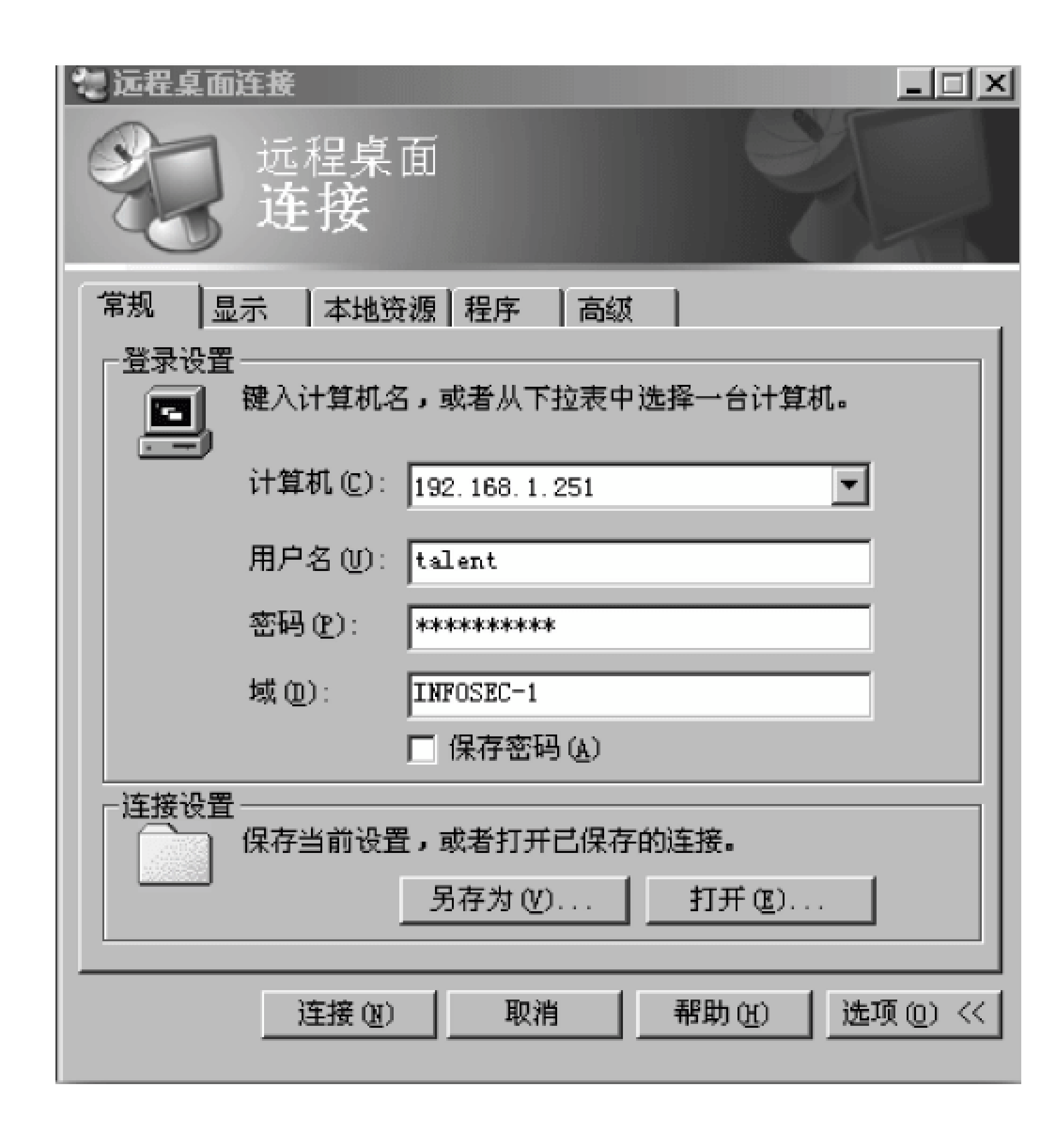


图1.9　远程连接到服务器

（4）如果连接成功，便会进入服务器窗口。

（5）右击桌面上的“网上邻居”图标，在快捷菜单中选择“属性”选项，然后在打开“网上邻居”窗口中的“本地连接”上右击，在快捷菜单中选择“属性”选项，在打开“本地链接属性”对话框中可以修改其IP地址吗？

（6）断开与服务器的连接，以用户名为“talent”和密码为“12345”，连续进行三次登录，会出现什么情况？

4. 思考题

在“本地策略”→“安全选项”中，有若干非常重要的安全设置，请挑选至少三个系统安全设置进行配置，并验证之。

实验2　系统漏洞扫描与评估

一、实验目的

使用漏洞扫描软件，对系统对象进行扫描、探测，获取目标系统的详细信息和漏洞，并试图加固系统。

二、实验原理

网络技术的飞速发展，网络规模迅猛增长和计算机系统日益复杂，导致新的系统漏洞层出不穷。由于系统管理员的疏忽或缺乏经验，导致旧的漏洞依然存在。许多人出于

好奇或别有用心，不停地窥视网上资源导致产生进行一次漏洞扫描的迫切性。因此需要采取外围的漏洞扫描系统机制来评估该系统的安全性，通过加固达到安全运行环境的目的。

三、实验内容

1. 实验环境

(1) 终端PC(Windows Server 2003系统)一台，打开多个端口，如Web、FTP、共享等，用于被扫描端。

(2) 软件工具：流光扫描工具。

(3) IIS、MSSQL等服务程序(账户密码较为简单，存在漏洞)作为扩充，非必要部署。

2. 实验角色

本实验为单人实验，每个人在各自的PC上进行实验操作。通过对本主机的漏洞扫描以及安全加固，对比加固前后的扫描报告。

3. 实验步骤

1) 浅层次扫描

(1) 在PC桌面上运行流光扫描软件。

(2) 设定扫描主机："文件"→"高级扫描向导"，打开设置对话框，"起始地址"和"结束地址"均设为127.0.0.1(本机)，单击"下一步"按钮，以后的设置均取默认值。直到出现如图1.10所示的"选择流光主机"对话框，单击"开始"按钮对本机进行扫描。



图1.10 "选择流光主机"对话框

(3) 开始扫描后，在右边的日志信息栏，显示扫描结果。

(4) 扫描结束后，系统询问"是否需要查看扫描报告?"，单击"是"按钮，显示扫描报告(注意记录扫描结果)。

2) 系统加固尝试

(1) 在终端PC中，执行"开始"→"运行"命令，在打开"运行"对话框中输入"services.msc"命令。

（2）单击“确定”按钮后，进入“服务”窗口，如图 1.11 所示。

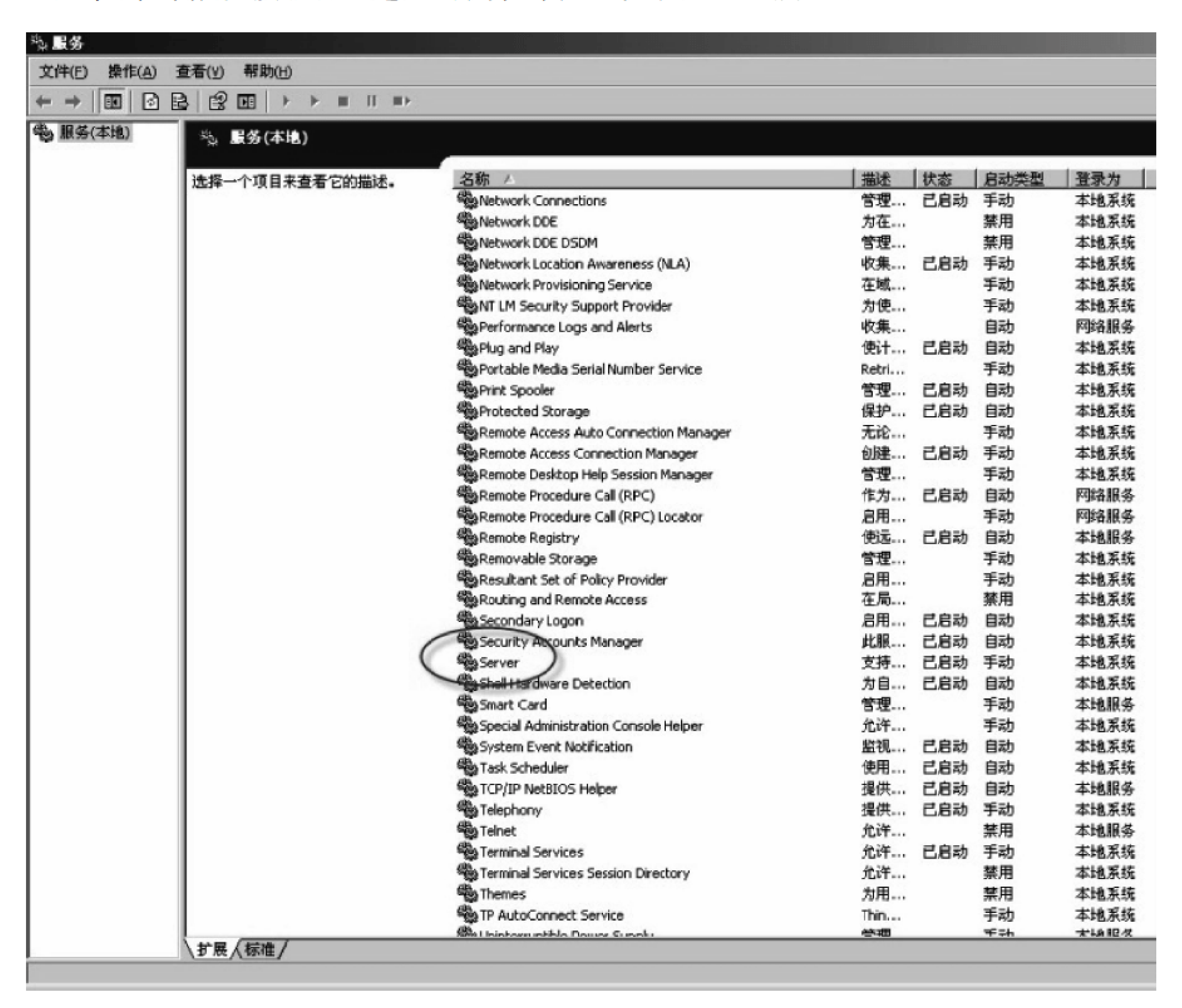


图 1.11　“服务”窗口

（3）在“服务”窗口中双击 Server 选项，并停止该服务，如图 1.12 所示。



图 1.12　停止 Server 服务

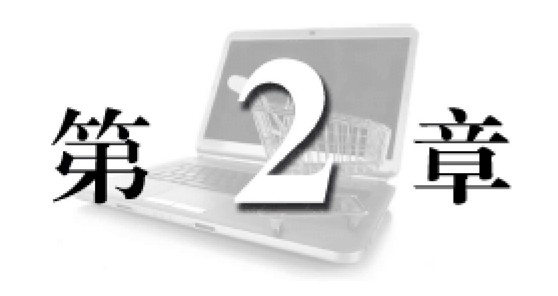
(4) 同样的方法,停止 Computer Browser 服务和 Distributed File System 服务。

3) 复查系统

重新启动流光扫描软件。注意扫描结果与上次扫描结果的不同。

4. 思考题

哪些系统特征可以被称为系统漏洞,如何发现?发现后,如何填补?

第章

网络系统安全篇

2.1 引言

随着信息化的普及和发展，互联网络已覆盖了社会政治、经济、文化、生活、生产的各个领域，网络安全也越来越成为全社会关注的焦点，并成为网络发展的重要课题。提高全社会网络安全意识，是保障我国信息化建设健康、稳定发展的长期重点工作之一。

网络安全是指保护网络中的硬件、软件及其系统不受偶然的或者恶意的破坏、更改、泄露，从而使系统以及网络服务连续、可靠、正常地运行。

从网络运行和管理者角度来说，人们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现"后门"、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。

网络安全系统包括防火墙、入侵检测与防护、病毒防护、内容安全、身份验证等部分构成。

2.2 网络安全

网络安全是一个综合的、动态的安全体系，它应该是多种安全技术的有机集成和安全产品之间的联动。"安全事件的意义不是局部的，将安全事件及时通告给相关的安全系统，有助于从全局范围评估安全事件的威胁，并在适当的位置采取动作。"这就是网络安全联动的理论基础。通过联动机制连接各功能模块，可以对各安全设备进行功能协调和实时监控，根据网络安全状况实现安全设备的配置和更改，把危害限制在最小范围内，产生"1＋1＞2"的合力，避免产生木桶效应。

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应

用数学、数论、信息论等多种学科的综合性学科，它涉及的因素主要包括物理安全、系统安全、信息安全和文件安全。国际标准化组织对计算机系统安全的定义是：为数据处理操作系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。

网络信息安全是一个系统性概念，是指为建立信息处理系统而采取的技术和管理上的安全保护。它包括了设备安全、自动化管理系统安全、各种数据安全、网络通信安全、管理维护安全、环境安全等几个方面，以保证信息的完整性、机密性、有效性、可控性和可审查性。信息的完整性是最基础的，它要求信息在存储、传递、提取整个过程中没有任何丢失或残缺现象；信息的机密性就是要求信息不被他人非法窃取或信息泄露；信息的有效性则是信息的一种真实性，要求信息能被准确无误地获得；信息的可控性则是指在网络范围内对信息具有控制的能力特性；信息的可审查性则是指信息交流过程结束后，交流双方要承认曾对信息的操作，不可否认做出合法或非法操作。所以要保障网络信息安全，就得从几个方面入手，首先是硬件安全，就是要保护网络硬件和媒体等设备不受自然损害；其次是软件安全，即计算机及其网络中各种软件不被篡改或破坏；最后是运行服务安全，即网络中各个网络系统要正常运行保证信息能顺畅地在各个网络系统中传递。

2.3 影响网络信息安全的因素

进入网络时代后，信息安全主要就是指网络信息安全。而网络信息的开放性、互联性使得网络信息有着很大的安全隐患。构成信息安全的因素可分为两类，一类是内部因素，一类是外部因素。内部因素包括硬件因素、软件因素。外部因素包括病毒、主动攻击、被动攻击、拒绝服务等方面。

1. 硬件因素

这类因素一方面是指受到自然环境对计算机网络设备与设施的影响，它具有突发性、自然性、不可抗拒性等特征，如因地震、风暴、洪水、雷击等自然威胁造成的系统运行异常；另一方面是指计算机设备被人为地损坏，出于各种利益盗取、破坏网络设备等。

2. 软件因素

这类因素主要是由计算机网络系统本身的缺陷漏洞造成的，因为系统本身没有及时采取有效的安全措施，如重要文件没有及时备份、共享文件没有保护、系统安全保护配置不合理等没有起到应有的作用造成网络信息安全受到威胁，系统安装软件或软件升级没有严格审核。

3. 病毒因素

病毒是主要的威胁信息安全因素，它主要侵害系统数据区、文件、内存、磁盘等区域，影响系统运行速度、干扰系统显示、降低系统运行效率等，对计算机系统造成严重影响，

甚至使得整个系统瘫痪。

4. 黑客攻击

在 Internet 上，黑客组织已经有了公开的网站，他们提供免费的黑客软件和一些黑客手段。当然，黑客攻击也分为两种：一种是破坏性活动；另一种是非破坏性活动。破坏性主要是指黑客以某种手段破坏信息的完整性及有效性；非破坏性就是黑客为了截获、窃取某些重要的信息，但是计算机还是能正常运行。黑客攻击是信息安全问题最为严重的一方面。

5. 拒绝服务因素

拒绝服务是指某些人不断地对服务器进行攻击、干扰使其不能正常工作，执行一些无关的程序，减慢系统运行速度，甚至崩溃无法运行，如 DOS 攻击。

6. 缓冲区溢出

这是系统中最容易受到攻击的漏洞。因为很多系统在不检查程序与缓冲区间的变化的情况下，就接收任意长度的数据，而把溢出部分存在堆栈里，然后系统照常执行命令。而留在堆栈里的数据就是破坏者有机可乘的入口，造成信息丢失或破坏。

2.4　网络信息安全措施

1. 防火墙技术

防火墙是将内部网和公众网访问相隔离以维护网络与信息安全的一种软件或硬件。防火墙包括有三种类型：数据包过滤路由器、应用层网关、电路层网关。防火墙位于内部网和与它相连的网络之间，在相互通信时进行控制，对信息进行监控保证信息安全。数据包过滤技术是根据系统内部设置的参数的过滤原则在网络层对数据包进行分析、选择，通过检查数据流中每一个数据包的源地址、目的地址、端口号、协议状态等参数来确定信息的安全性，是否允许数据通过。对不符合规则的数据包拦截下来，包过滤规则主要还是根据 IP 信息来判断，由于 TCP/IP 协议本身存在漏洞，所以有时也会因为假 IP 地址而出现信息错误。

2. 访问控制技术

访问控制包括两方面，一方面是控制人员登录，对其进行身份验证。身份验证主要包括验证依据，它可以是用户名、密码等验证，还可以根据身体特征如指纹、声音等要素进行身份验证，这样可以防止非管理人员进入到管理员界面进行非法操作，如浏览不属其权限范围的文件、网页及数据。另一方面是存取控制，存取控制是指特定人员对特定事物的存取权限限制，主要包括人员限制、数据标识、权限控制等。它一般与身份验证一起使用，赋予不同的用户不同的权限，对不同对象享有不同的操作，使得信息分层管理，一定程度上对信息的安全性有了保障。

3．信息加密技术

对信息进行加密可以在很大程度上保护信息。在计算机网络中，数据传输可能涉及多台主机，可能经过不可信网络系统，所以采用加密手段对保护信息实现网络安全是十分重要的。防止有人在中途截取信息，对信息进行修改、删除、泄露、篡改、破坏等行为，也可以防止非管理人员对信息进行分析而损害信息终端的使用者。数据加密一般分为三个层次的加密：链路加密、字节加密和端到端加密。

4．数字签名技术

数字签名是附加在传输的数据上跟数据一起传输的一串代码，通过一个函数对要传送的报文进行处理用以认证报文的来源并核实报文是否发生更改，提供了一种鉴别方法，解决传输过程中信息的伪造、抵赖和冒充等安全问题。发送者利用只有自己知道的私钥进行加密，得到数字签名，然后再加入到要传送的数据中。这样就可以防止在中途信息被截而被篡改。接收者在收到信息时先解密再使用数据。现在流行的电子交易中经常用到数字签名技术来保证交易的顺利进行。

2.5 公钥体系

随着网络应用的蓬勃发展，特别是电子商务、电子政务、远程教育等的兴起，网络安全越来越受到重视。学术界和有关厂商经过多年的研究之后，初步形成了一套完整的解决方案，即公钥基础设施。

1．身份认证

身份认证是实现网络安全的重要机制，是其他安全机制的基础。只有实现了有效的身份认证，才能保证访问控制、安全审计等安全机制的有效实施。在PKI（Public Key Infrastructure，公钥基础设施）系统中，通过公钥证书来确认用户的身份，其实质是利用了公钥密码理论的特点。在双方进行通信时，要验证单方或双方的身份。在证书的使用者和证书的主体之间建立一个证书的可信任路径，认证路径中每一个证书的签名，验证每一个证书的有效性，即在给定期间内没有被注销也没有过期。认证中心CA（Certificate Authority）在公钥证书中的数字签名，有效防止了证书的伪造和篡改。本模型中的身份认证功能由PKI安全应用支撑平台来提供。

2．公钥证书（Public Key Certificate）

公钥证书是由CA颁发并经CA数字签名的，包含公开密钥拥有者以及公开密钥相关信息的一种电子文件，可以用来证明公钥证书持有者的真实身份。证书的格式遵循ITU-T X.509国际标准。需要特别提到的是，公钥证书中的扩展域，一个扩展域包括重要性标志（Criticality Flag）和与标志的扩展域有关的ASN.1类型数据值的编码。具体扩展可以根据ITU-T标准来定义，或者是由任何组织自己来定义所需的扩展，也就是说，可以将自己所需的特定信息以扩展域形式编进证书中，以满足特定应用的需求，因

此,将用户的角色信息作为证书的一项扩展域而存储在证书中,提供对权限管理的支持。

3. PKI

PKI是基于公钥密码理论的技术体系,可以作为支持认证、完整性、机密性和不可否认性的技术基础。它能够为所有网络应用提供密钥和证书的集中化管理,从而为用户提供身份认证和安全通信等服务。PKI包括这样几个部分:用于用户注册和接受用户证书请求的注册机RA(Register Authority);负责生成密钥、发放和管理证书的权威机构CA;对密钥、证书及证书撤销列表的存储和管理的目录服务器(Directory);在密钥丢失时,进行密钥恢复和实现密钥存储与管理的密钥管理系统;实现对整个PKI系统的控制和管理的模块。在该体系中,CA是核心机构,与公钥证书共同实现对身份认证的支持。

4. 访问控制模型

常见的访问控制策略有自主访问控制(DAC)、强制访问控制(MAC)以及基于角色的访问控制(RBAC)等。ITU-T的X.812访问控制框架定义了访问控制授权方案的抽象模型。应用于B/S模式时,主要由实施机制参考策略来决定用户请求的结果。基于角色的访问控制(Role Based Access Control)方法主要通过角色分层(Role Hierarchies)、责任分离(Separation of Duty)等技术将权限与用户分离来简化安全管理。基本思想是将访问许可权分配给一定的角色,用户通过饰演不同的角色获得角色所拥有的访问许可权。角色成为访问控制中访问主体和受控对象之间的中介。访问控制机制是在用户和受控资源之间介入的一个安全机制,用来验证用户权限、控制对受控资源的访问。

5. XML技术

XML(eXtensible Markup Language)技术曾经有力地促进了Internet发展的HTLM语言,由于其存在难以扩展、交互性差、语义性差等缺点,阻碍了其更广泛的应用。XML SGML(Standard Generalized Markup Language)的丰富功能与HTML的易用性结合到Web中,以一种开放的自我描述方式定义了数据结构,在描述数据内容的同时能突出对结构的描述,从而体现出数据之间的关系,成为描述数据和交换数据的标准格式。更重要的是,XML允许组织、个人建立适合自己需要的标志集合。利用XML技术,可以很方便地定义符合特定需要的数据格式。本模型中,将需要保护的资源对象(Object)、用户的角色(Role)和访问方法(Method)以XML结点形式存储,增强了系统的灵活性和可操作性,同时还方便了开发人员的编程。XML存储了访问控制策略信息。

2.6 Adobe Acrobat 软件概述

Adobe Acrobat软件是美国Adobe公司跨平台信息共享的重要工具,可以将电子表单、网页文件、MSOffice文件等数十种格式的文件完美地转换为便携式文档格式(PDF),

并保留源文档的字体、图像、图形和版面设置。从20世纪90年代以来，随着因特网技术的飞速发展，PDF文件已成为文档电子交换的事实标准，政府部门、企业及教育机构中也越来越多地通过使用PDF电子信息交换工作流替代基于纸张的工作流来简化操作流程。

2.7 网络流量监测

1. 网络流量的特性

通过对互联网通信量的测量，人们发现互联网通信量的主要特性如下：

（1）数据流是双向的，但通常是非对称的。互联网上大部分的应用都是双向交换数据的，因此网络的数据流是双向的。但是两个方向上的数据率有很大的差异，这是因为从网站下载时会导致从网站到客户端方向的数据量比另外一个方向多。

（2）大部分TCP会话是短期的。超过90%的TCP会话交换的数据量小于10KB，会话持续时间不超过几秒。虽然文件传输和远程登录这些TCP会话都不是短期的，但是由于80%的WWW文件传输都小于10KB，WWW的巨大增长使其在这方面产生了决定性的影响。

（3）包的到达过程不是泊松过程。大部分传统的排队理论和通信网络设计都假设包的到达过程是泊松过程，即包到达的时间的分布是独立的指数分布。简单地说，泊松到达过程就是事件（如地震、交通事故、电话等）按照一定的概率独立的发生。泊松模型因为指数分布的无记忆性也就是事件之间的非相关性而使其在应用上要比其他模型更加简单。然而近年来对互联网络通信量的测量显示包到达的过程不是泊松过程。包到达的时间不仅不服从指数分布，而且不是独立分布的。大部分时候是多个包连续到达，即包的到达是有突发性的。很明显，泊松过程不足以精确地描述包的到达过程。造成这种非泊松结构的部分原因是数据传输所使用的协议。非泊松过程的现象迫使人们怀疑使用简单的泊松模型研究网络的可靠性，从而促进了网络通信量模型的研究。

（4）网络通信量具有局域性。互联网流量的局域性包括时间局域性和空间局域性。用户在应用层对互联网的访问反映在包的时间和源及目的地址上，从而显示出基于时间的相关（时间局域性）和基于空间的相关（空间局域性）。

2. 网络流量的测量

网络流量的测量是人们研究互联网络的一个工具，通过采集和分析互联网的数据流，我们可以设计出更加符合实际的网络设备和更加合理的网络协议。计算机网络不是永远不会出错的，设备的一小点故障都有可能使整个网络瘫痪，或者使网络性能明显下降。例如，广播风暴、非法包长、错误地址、安全攻击等。对互联网流量的测量可以为网络管理者提供详细的信息，以帮助发现和解决问题。互联网流量的测量从不同的方面可以分为以下几种：

（1）基于硬件的测量和基于软件的测量。基于硬件的测量通常指使用为采集和分析网络数据而特别设计的专用硬件设备进行网络流的测量，这些设备一般都比较昂贵，而且受网络接口数量、网络插件的类型、存储能力和协议分析能力等诸多因素的限制。基于软件的测量通常依靠修改工作站的内核中的网络接口部分，使其具备捕获网络数据包的功能。与基于硬件的方法比较，其费用比较低廉，但是性能比不上专用的网络流量分析器。

（2）主动测量和被动测量。被动测量只是记录网络的数据流，不向网络流中注入任何数据。大部分网络流量测量都是被动的测量。主动测量使用由测量设备产生的数据流来探测网络而获知网络的信息。例如，使用 ping 来估计到某个目的地址的网络延时。

（3）在线分析和离线分析。有的网络流量分析器支持实时地收集和分析网络数据，使用可视化手段在线地显示流量数据和分析结果，大部分基于硬件的网络分析器都具有这个能力。离线分析只是在线地收集网络数据，把数据存储下来，并不对数据进行实时的分析。

（4）协议级分类。对于不同的协议，如以太网（Ethernet）、帧中继（FrameRelay）、异步传输模式（Asynchronous Transfer Mode），需要使用不同的网络插件来收集网络数据，因此也就有了不同的通信量测试方法。

3. 网络流量的监测技术

根据对网络流量的采集方式可将网络流量监测技术分为基于网络流量全镜像的监测技术、基于 SNMP 的监测技术和基于 Netflow 的监测技术三种常用技术。

（1）基于网络流量全镜像的监测技术：网络流量全镜像采集是目前 IDS 主要采用的网络流量采集模式。其原理是通过交换机等网络设备的端口镜像或者通过分光器、网络探针等附加设备，实现网络流量的无损复制和镜像采集。和其他两种流量采集方式相比，网络流量全镜像采集的最大特点是能够提供丰富的应用层信息。

（2）基于 Netflow 的流量监测技术：Netflow 流量信息采集是基于网络设备提供的 Netflow 机制实现的网络流量信息采集。

（3）基于 SNMP 的流量监测技术：基于 SNMP 的流量信息采集，实质上是通过提取网络设备 Agent 提供的 MIB（管理对象信息库）中收集一些具体设备及流量信息有关的变量。基于 SNMP 收集的网络流量信息包括：输入字节数、输入非广播包数、输入广播包数、输入包丢弃数、输入包错误数、输入未知协议包数、输出字节数、输出非广播包数、输出广播包数、输出包丢弃数、输出包错误数、输出队长等。在此基础上实现的流量信息采集效率和效果均能够满足网络流量监测的需求。

表 2.1 对三种网络流量监测技术进行了综合比较，不难得出以下结论：基于 SNMP 的流量监测技术能够满足网络流量分析的需要，且信息采集效率高，适合在各类网络中应用。

表 2.1 三种网络流量监测技术比较

	万全流量镜像	SNMP	Netflow
标准化情况	不完全标准	RFC 标准	有望成为 RFC 标准
设备支持能力	端口流量镜像方式的使用范围有限。若采用探针方式，则与探针自身的功能、性能有关	广泛支持	Cisco、Juniper、Foundry 三个主流厂家的设备支持
是否需要采样	否	否	可能
是否含 AS 信息	否	否	是
数据粒度	细	粗	中
数据准确性	准确	准确	统计意义上的准确
支持的数据容量	大	小	大
对网络影响	端口镜像模式影响较大：探针方式安装时影响较大，一旦安装后影响较小，但带来新的单点失效点	小	小
部署难度	较大	小	小
部署成本	高	低	低
适用范围	接入层/汇聚层	网络各个层次	汇聚层/核心层

实验 3 Adobe Acrobat 中的公钥证书配置

一、实验目的

理解数字证书的含义及其实现原理，并掌握在 Adobe Acrobat 中利用公钥证书配置安全性策略的方法。

二、实验原理

数字证书是一种能提供在 Internet 上进行身份验证的一种权威性电子文档，人们可以在互联网交往中用它来证明自己的身份和识别对方的身份。

以数字证书为核心的加密技术可以对网络上传输的信息进行加密和解密、数字签名和签名验证，确保网上传递信息的机密性、完整性。使用了数字证书，即使发送的信息在网上被他人截获，甚至丢失了个人的账户、密码等信息，仍可以保证用户的账户、资金安全。

使用证书加密文档并验证数字签名。数字签名可使收件人确信文档来自发件人处。加密确保仅有预期的收件人可以查看内容。证书是可存储数字身份证的公钥组件。

当用证书保护 PDF 文档时，可指定收件人并定义每个收件人或组的文件访问级别。例如，可以允许一组签名和填写表单，允许另一组编辑文本或删除页面。可以从自己的可信任身份列表、磁盘上的文件、LDAP 服务器或 Windows 证书储存区（仅 Windows）来选择证书。总是将自己的证书包含在收件人列表，以便稍后可以打开文档。

注意：*如果可能，请使用第三方数字身份证的证书加密文档。如果证书丢失或被盗，颁发机构可以进行替换。如果自签名数字身份证被删除，使用该身份证的证书加密的所有 PDF 将永远无法访问。*

三、实验内容

1. 实验环境

（1）硬件设备：部署 Windows Server 2003 系统的学生 PC 一台。

（2）软件工具：Adobe Acrobat 9.3.3 ProExtended。

2. 实验角色

本实验为单人实验，每个人在各自的PC终端上进行实验操作。实验工具已预先安装好。

3. 实验步骤

（1）新建一个Word文件，内容任意，以文件名“test.doc”存盘（注意该文件的保存位置）。

（2）打开实验软件。执行“开始”→“所有程序”→“Acrobat”→“Adobe Acrobat 9 ProExtended”命令。

（3）选择“文件”→“创建PDF”→“从文件”选项，在打开的窗口中，选择文件“test.doc”，创建pdf文件（创建pdf文件可能需要一段时间，请耐心等待。文件创建完成后，系统自动为其命名test.pdf）。

（4）选择“文件”→“保存”选项，将文件以test.pdf为文件名保存到磁盘上。

（5）选择“高级”→“安全性”→“管理安全性策略”选项，打开“管理安全性策略”对话框，在该对话框中单击“新建”按钮，打开“新建安全性策略”对话框，如图2.1所示。



图2.1 “新建安全性策略”对话框

(6) 在“策略名称”栏中填写为该安全策略取的名字(可自行填写);在“说明”栏填写班级、姓名和学号;在“选择要加密的文档组件”选项区域中,选中“加密所有文档内容”单选按钮,其他默认(注意分析其他几个选项的含义),单击“下一步”按钮。

(7) 在弹出如图 2.2 所示的对话框中,单击“添加数字身份证”按钮,选择“我要立即创建新数字身份证”选项,然后单击“下一步”按钮。

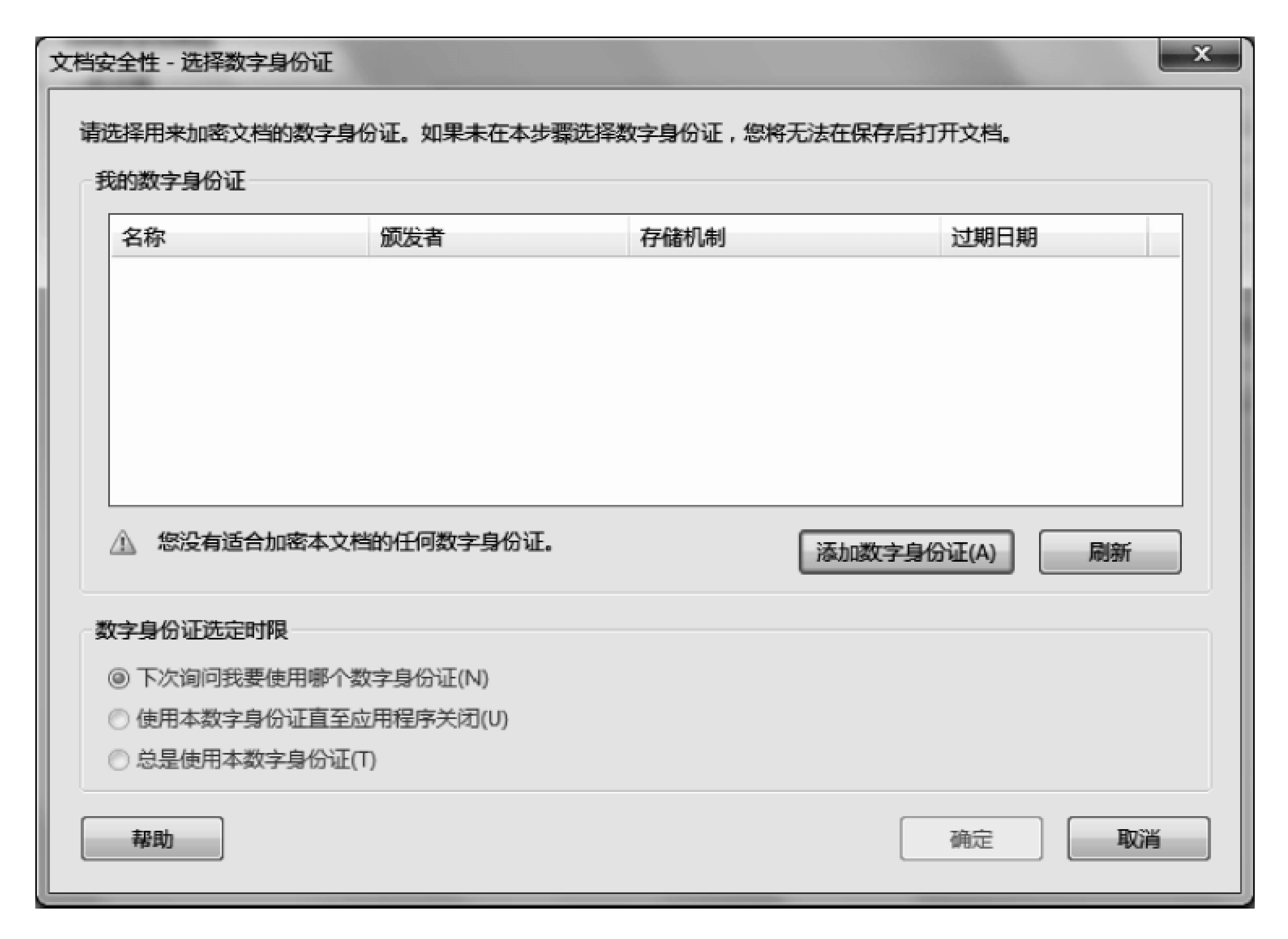


图 2.2　选择数字身份证

(8) 在弹出如图 2.3 所示的对话框中,选中 “新建 PKCS＃12 数字身份证文件”单选按钮,单击“下一步”按钮。



图 2.3　添加数字身份证

(9) 在弹出如图 2.4 所示的对话框中，填入相关信息(名称，你的姓名；部门，你的专业名称；单位名称，上海商学院；电子邮件地址，你的电子邮件地址；国家/地区，中国；其余取默认值)，单击“下一步”按钮。

添加数字身份证

输入要在生成自签名证书时使用的身份信息。

名称（例如：John Smith）(M)：张新谊

部门(U)：计算机学院

单位名称(O)：上海商学院

电子邮件地址(E)：61xinyi@163.com

国家 / 地区(C)：CN - 中国

启用 Unicode 支持(A)

密钥算法(K)：1024-bit RSA

数字身份证用于(F)：数字签名和数据加密

取消　< 上一步(B)　下一步(N) >

图 2.4　填写身份信息

注意：以上信息，如果填写的是中文，单击“下一步”按钮后，系统会出现如图 2.5 所示的兼容性警告，单击“是”按钮，将以上信息以 ASCII 的形式重新输入，如图 2.6 所示。

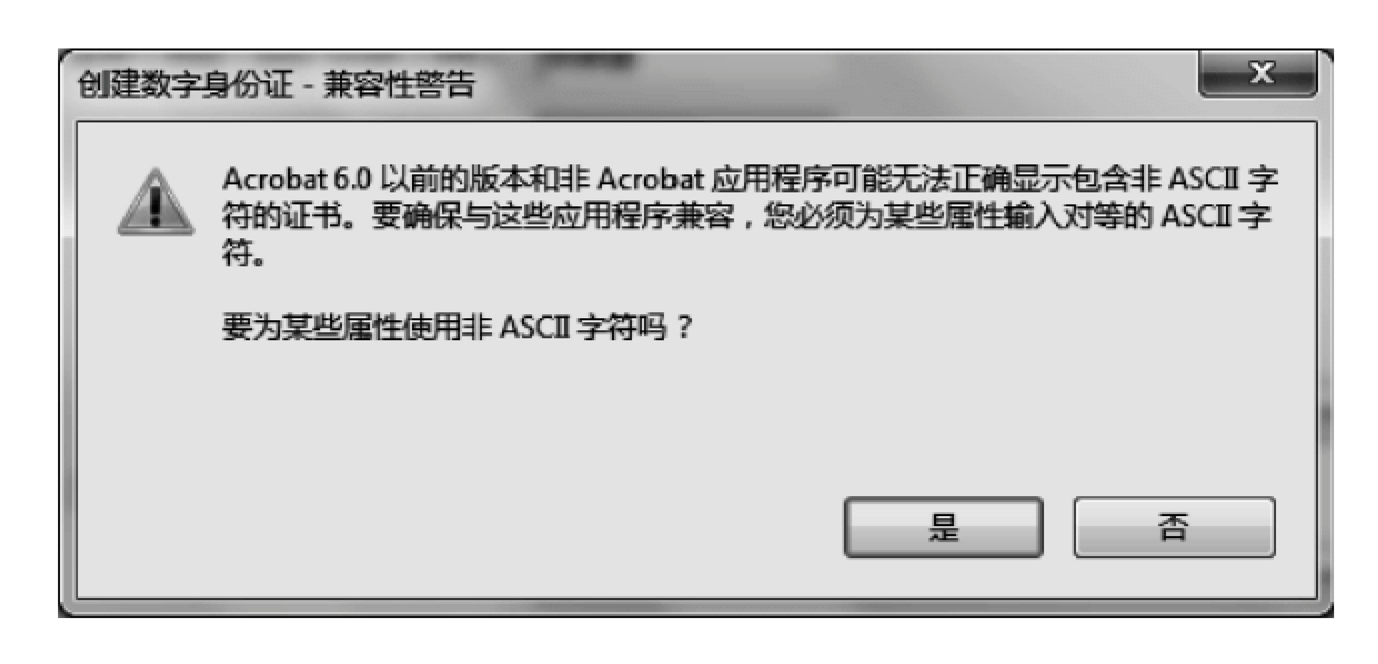


图 2.5　兼容性警告

(10) 在弹出如图 2.7 所示的对话框中输入口令为“123456”，其余取默认值，单击“完成”按钮。

(11) 关闭“文档安全性-选择数字认证”对话框，返回“管理安全性策略”对话框，如图 2.8 所示。选择新建的数字身份证为收件人，然后单击“应用到文档”按钮。将所创建的 pdf 文档以 test1. pdf 为保存，关闭该软件。



图 2.6 以 ASCII 形式重新输入



图 2.7 填写口令



图 2.8　安全策略应用到文档

(12) 重新打开 test1. pdf 文档，将出现如图 2.9 所示的“数字身份证验证”对话框，可查看该数字身份证信息是否是之前设置的信息(图 2.10)。输入之前设置的口令为“123456”，将打开 test1. pdf 文件。



图 2.9　数字身份证验证

(13) 因为之前没有设置对该 pdf 文档的具体的编辑权限限制，因此选择“工具”→“高级编辑”选项，可以对该文档进行添加按钮、裁剪、复制等操作，如图 2.11 所示。

(14) 选择“高级”→“安全性”→“管理安全性策略”选项，在出现的“管理安全性策略”对话框中选择“test”策略，然后单击“编辑”按钮，如图 2.12 所示。

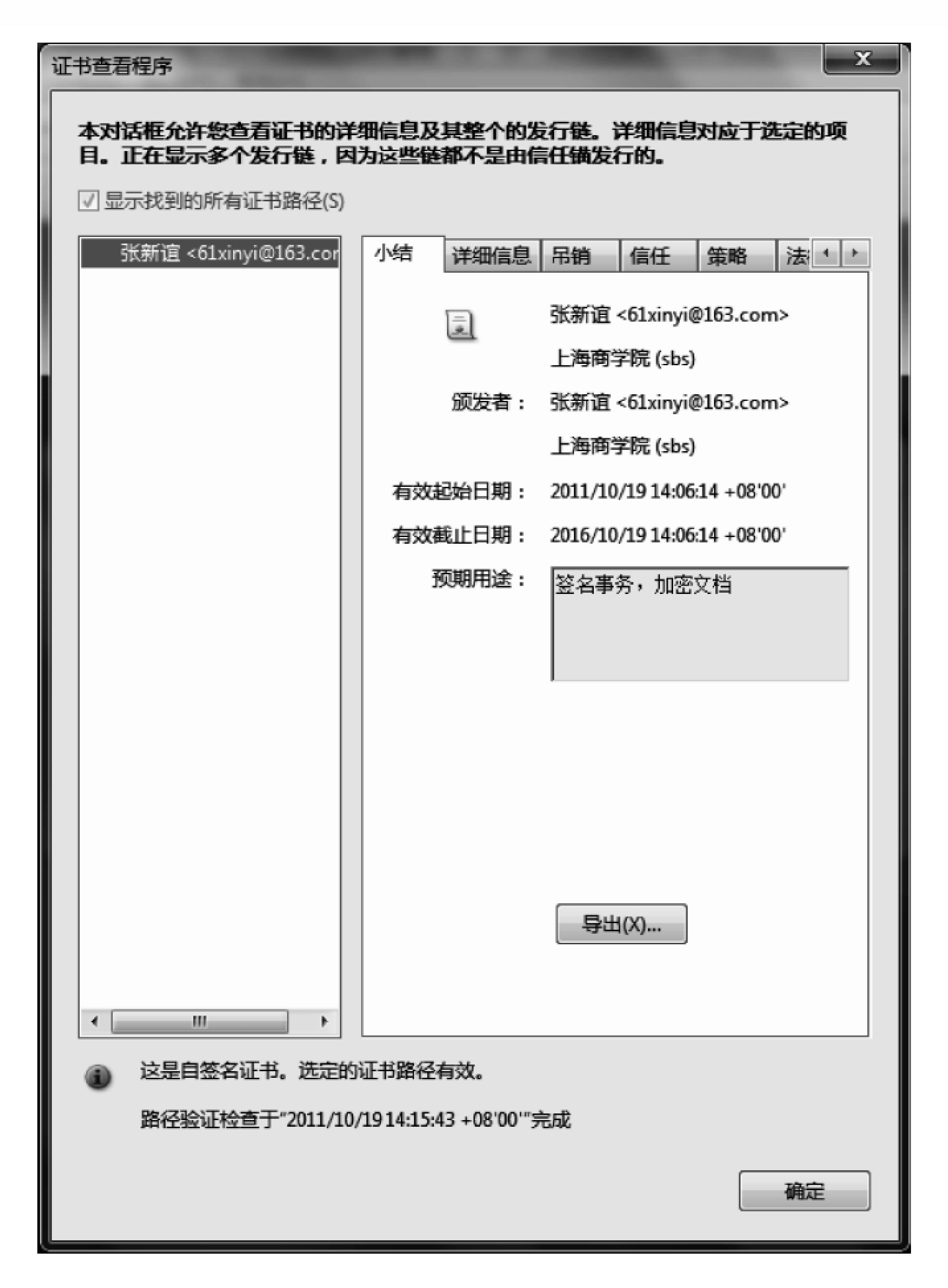


图 2.10　证书详细信息



图 2.11　文档的编辑权限



图 2.12　选择加密证书

(15) 安全证书的一般设置,如图 2.13 所示,单击“下一步”按钮。



图 2.13　安全证书的一般设置

(16) 在弹出如图 2.14 所示的对话框中,单击“许可”按钮,在出现的“许可设置”对话框中选中“限制文档的打印和编辑及其安全性设置”复选框,可更改文档的打印权限、编辑权限等,设置如图 2.15 所示。然后依次单击“确定”→“下一步”→“完成”→“应用到文档”按钮,将文档以 test2.pdf 保存。

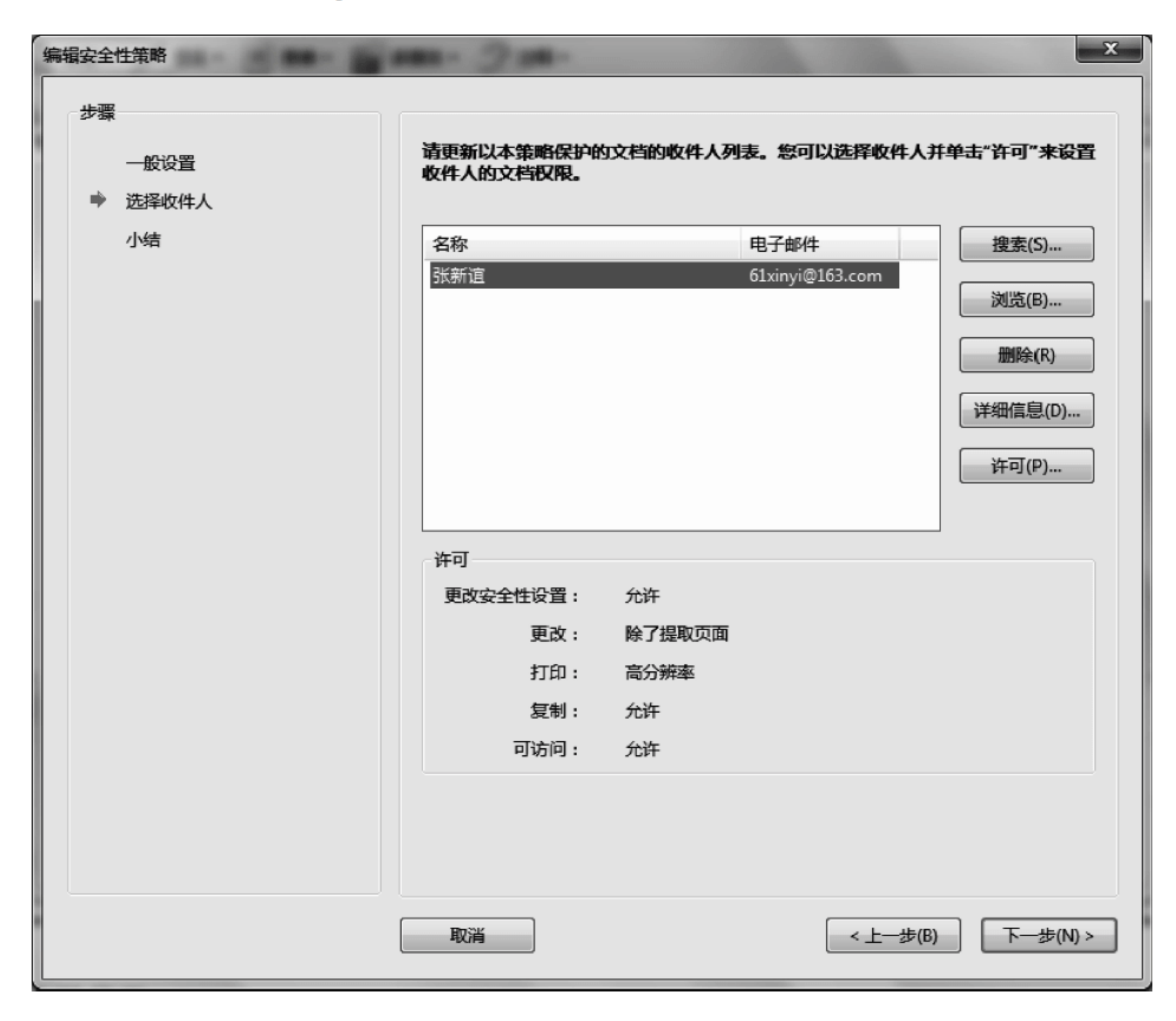


图 2.14 当前的安全设定信息

(17) 关闭该 pdf 文档,然后重新打开 test2.pdf 文档,选择“工具”→“高级编辑”选项,发现好多修改工具已成灰色,不可用,如图 2.16 所示。

4. 思考题

(1) 本实验生成的三个文件:test.pdf、test1.pdf、test2.pdf 有什么区别?

(2) 大家测试一下,如果创建的数字身份证被删除,还能够打开原来经该数字身份证签名的文件吗?

(3) 为了保护我们的著作权,需要设置一篇文章只能被别人网上查阅,不能修改,不能复制,不能打印,该如何设置安全性策略呢?

(4) 通过该实验,你能说出数字签名与公钥证书的工作原理吗?



图 2.15　重设安全许可



图 2.16　编辑功能受限

实验 4　网络流量监测与分析

一、实验目的

通过抓包工具 Wireshark，抓取 telent、ssh 包，完成对 telnet 包的分析工作，明白 telnet 包的结构，结合 TCP/IP 五层模型，分析 telnet 包各层的功能，以及各层通信使用

的地址，通过 telent 包的测试了解并且分析数据包中登录密码等信息和了解明文传输的特点，并且通过对 ssh 包的测试来了解密文传输的安全性。

二、实验原理

Telnet 协议是 TCP/IP 协议族中的一员，是 Internet 远程登录服务的标准协议和主要方式，它为用户提供了在本地计算机上完成远程主机工作的能力。在终端使用者的计算机上使用 Telnet 程序，用它连接到服务器。终端使用者可以在 Telnet 程序中输入命令，这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样，可以在本地就能控制服务器。要开始一个 Telnet 会话，必须输入用户名和密码来登录服务器。Telnet 是常用的远程控制服务器的方法。

使用 Telnet 协议进行远程登录时需要满足以下条件：在本地计算机上必须装有包含 Telnet 协议的客户程序；必须知道远程主机的 IP 地址或域名；必须知道登录标识与口令。

Telnet 远程登录服务分为以下 4 个过程：

(1) 本地与远程主机建立连接。该过程实际上是建立一个 TCP 连接，用户必须知道远程主机的 IP 地址或域名。

(2) 将本地终端上输入的用户名和口令及以后输入的任何命令或字符以 NVT(Net Virtual Terminal)格式传送到远程主机。该过程实际上是从本地主机向远程主机发送一个 IP 数据包。

(3) 将远程主机输出的 NVT 格式的数据转化为本地所接受的格式送回本地终端，包括输入命令回显和命令执行结果。

(4) 本地终端对远程主机进行撤销连接。该过程是撤销一个 TCP 连接。

SSH 是 Secure Shell 的缩写，由 IETF 的网络工作小组(Network Working Group)所制定；SSH 为建立在应用层和传输层基础上的安全协议。SSH 是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。

传统的网络服务程序，如 ftp、pop 和 telnet 在本质上都是不安全的，因为它们在网络上用明文传送口令和数据，别有用心的人非常容易就可以截获这些口令和数据。而且，这些服务程序的安全验证方式也是有其弱点的，就是很容易受到“中间人”(man-in-the-middle)的攻击。所谓“中间人”攻击方式，就是“中间人”冒充真正的服务器接收你传给服务器的数据，然后再冒充你把数据传给真正的服务器。服务器和你之间的数据传送被“中间人”一转手做了手脚之后，就会出现很严重的问题。

通过使用 SSH，你可以把所有传输的数据进行加密，这样“中间人”攻击方式就不可能实现了，而且也能够防止 DNS 和 IP 欺骗。还有一个额外的好处就是传输的数据是经过压缩的，所以可以加快传输的速度。SSH 有很多功能，它既可以代替 telnet，又可以为 ftp、pop、甚至 ppp 提供一个安全的“通道”。

三、实验内容

1. 实验环境

(1) 硬件设备：Windows Server 2003 系统的学生 PC 一台；RHEL 系统的服务器一台。

(2) 软件工具：Wireshark；IE 6.0。

实验拓扑图和实验设备配置参考信息分别如图 2.17 和表 2.2 所示。

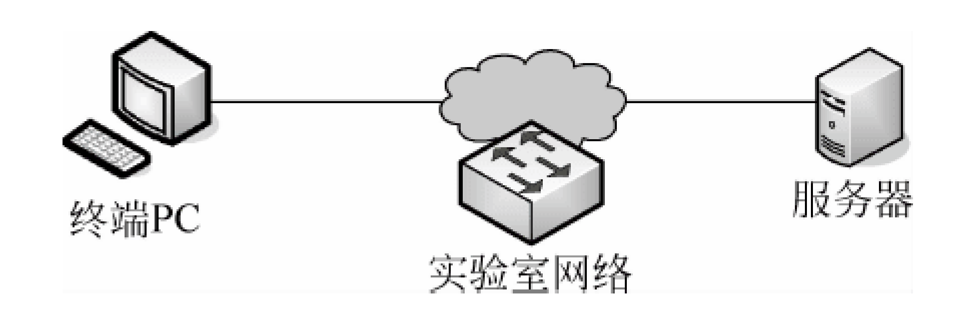


图 2.17　实验拓扑图

表 2.2　实验设备配置参考信息表

设 备 名 称	IP 地址
示例实验终端 PC	192.168.1.100
RHEL5 系统的服务器	192.168.1.252

2. 实验角色

本实验为单人实验，每个人在各自的 PC 终端上进行试验操作。通过对服务器进行 telnet 和 ssh 登录的过程中进行抓包分析，了解明文、密文传输对于账户和密码安全的区别，从而学习抓包的基本能力以及对 IP 包的深入解析和学习。

本实验需要通过网络进行包抓取和分析，因此实验环境必须 Ping 协议可用，telnet，ssh 服务可用，方可保证实验的可行性。

3. 实验步骤

1) telnet 包检测

(1) 打开抓包工具 Wireshark，在过滤框中输入 telnet 过滤 telnet 包，启动程序并抓包。

提示：

一般地讲，该工具会识别出多个物理网卡及逻辑网口，因此请选择实际 PC 主机上的试验用的物理网卡作为抓包接口对象，也可以根据 IP 地址来判断哪个 IP 是抓包对象。上例中仅作为说明，选择其中一块试验用的网卡进行抓包。

(2) 执行“开始”→“运行”命令，在打开的“运行”对话框中输入 cmd 命令，打开命令行窗口，输入 IPCONFIG 命令，记录本机的 IP 地址。

(3) 在命令窗口中输入：Ping 192.168.1.252，注意连接是否正常。

(4) 在命令窗口中输入：telnet 192.168.1.252，登录服务器。登录账户和密码均为 gengshang，成功后提示符为 $ 。

(5) 此时，抓包的具体信息开始有记录信息了，系统成功获取包信息如图 2.18 所示。

(6) 从图 2.19 中看到 telnet 的请求和响应报文，现在抓取 telnet 报文分析如下。

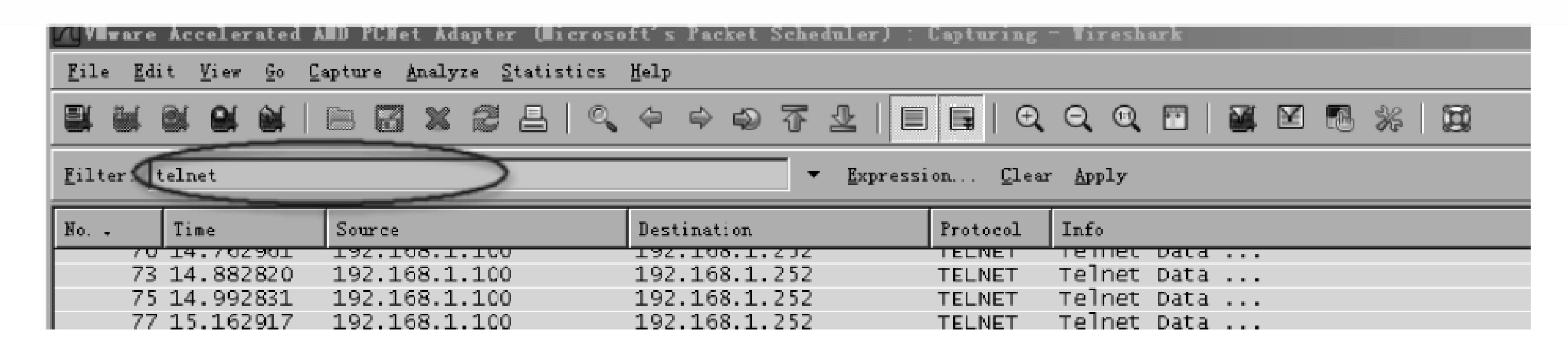


图 2.18 抓包信息

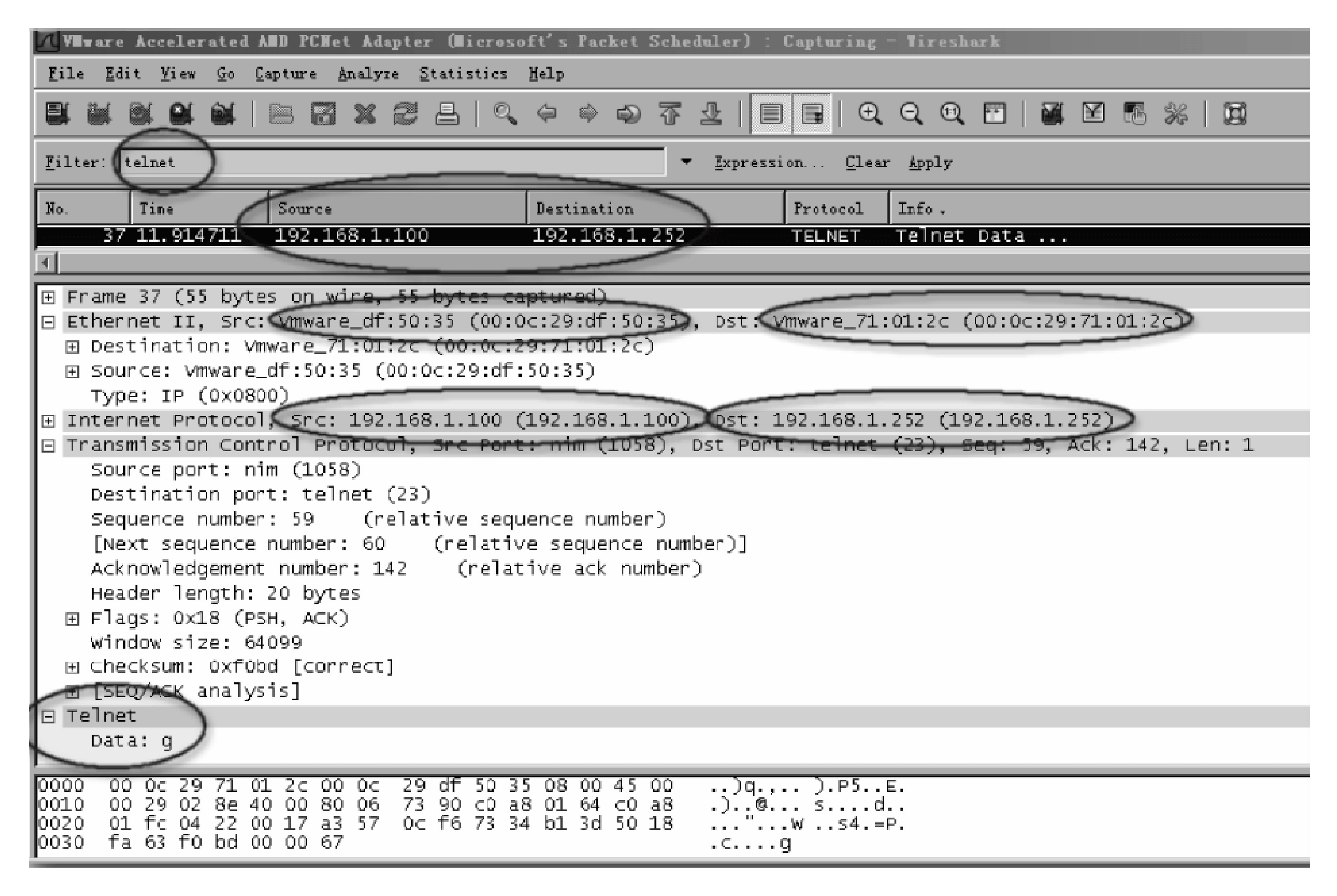


图 2.19 报文信息

二层参数：在列表 Ethernet II 部分，指示底层的环境是以太网，协议包中 Ethernet II 型参数给出本机和测试目标主机的二层地址，即 MAC 地址。因为 telnetre quest 包是从本地 PC 发给测试目标 PC 的，所以这里的 Src(源 MAC 地址)就是本机网卡的 MAC 地址，在本实验中是 00：0C：29：df：50：35，而 Dst(目标 MAC 地址)在本实验环境下也就是服务器的 MAC 地址。

三层参数：在列表 Internet Protocol 部分，给出测试包的源 IPv4 地址和目标 IPv4 地址，其中源 IP 地址(本地主机)为 192.168.1.100；目标 IP 地址(测试主机的 IP 地址)为 192.168.1.252。

高层参数：在列表 Internet Control Message Protocol 中，显示目标端口 23。

telnet 参数：客户机 192.168.1.100 是在 telnet 登录 192.168.1.252 时输入的账户及密码(gengshang)，因为 telnet 时双方的数据包是明文显示的。

(7) 选择 Analyze→Follow TCP Stream 选项，在打开的窗口中显示报文信息，如图 2.20 所示。

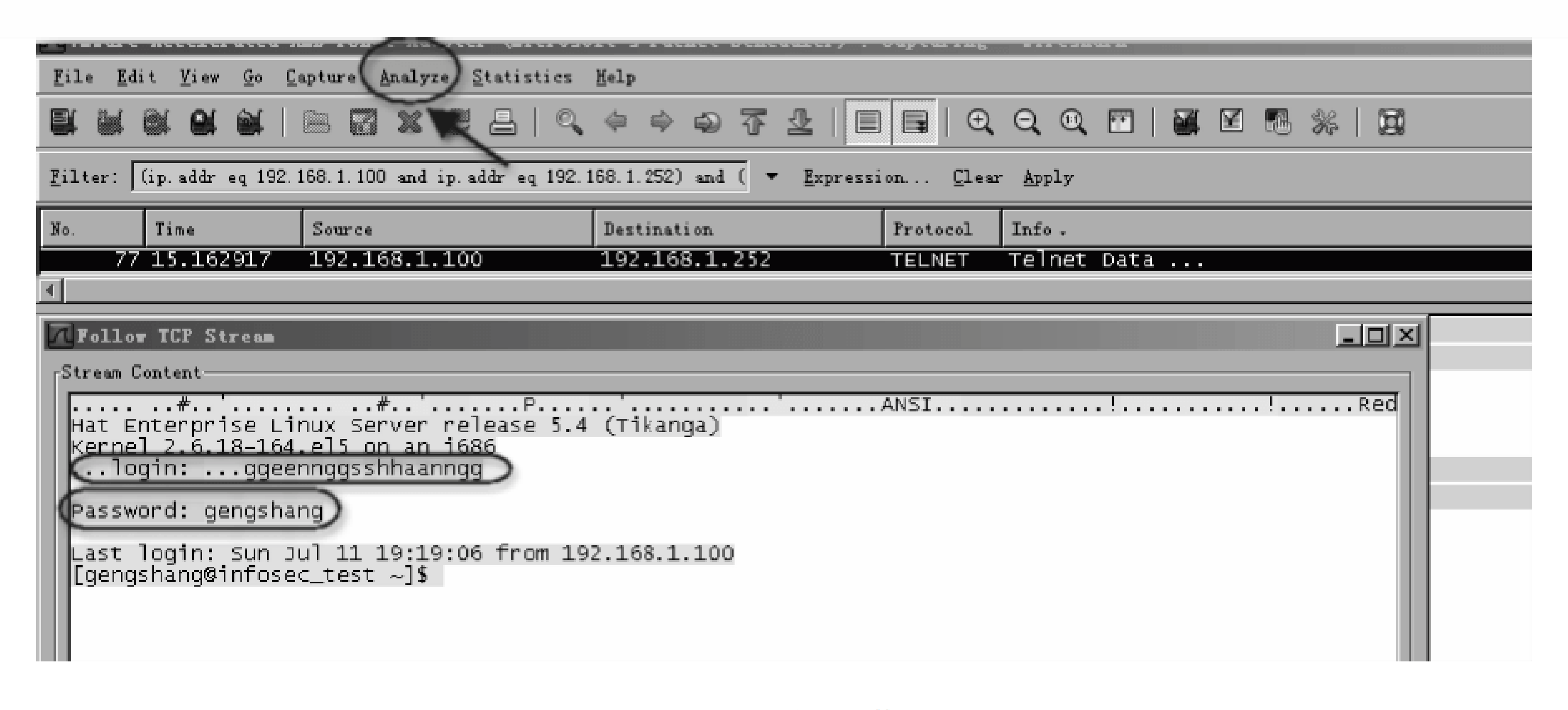


图 2.20　报文信息

从图 2.20 中也可以直接看到 telnet 过程中，由于是明文传输因此抓包工具可以直接的捕获其中的用户名和密码，输入账户时通过网卡时被抓包，抓包软件显示抓到一次账户名。当服务器再次确认用户名时回显在终端 PC 时，抓包工具再一次显示抓到一次账户名，因此有 ggeenngg sshhaanngg 重复的出现。而根据 telnet 协议中密码不再回显，所以抓包工具只能抓到终端输入密码而没有服务器再次确认密码。

2）ssh 包检测

(1) 单击桌面 PuTTY 图标。

(2) 打开 PuTTY，并输入服务器 IP 地址 192.168.1.252，选择 SSH 登录，最后单击 Open 按钮，如图 2.21 所示。

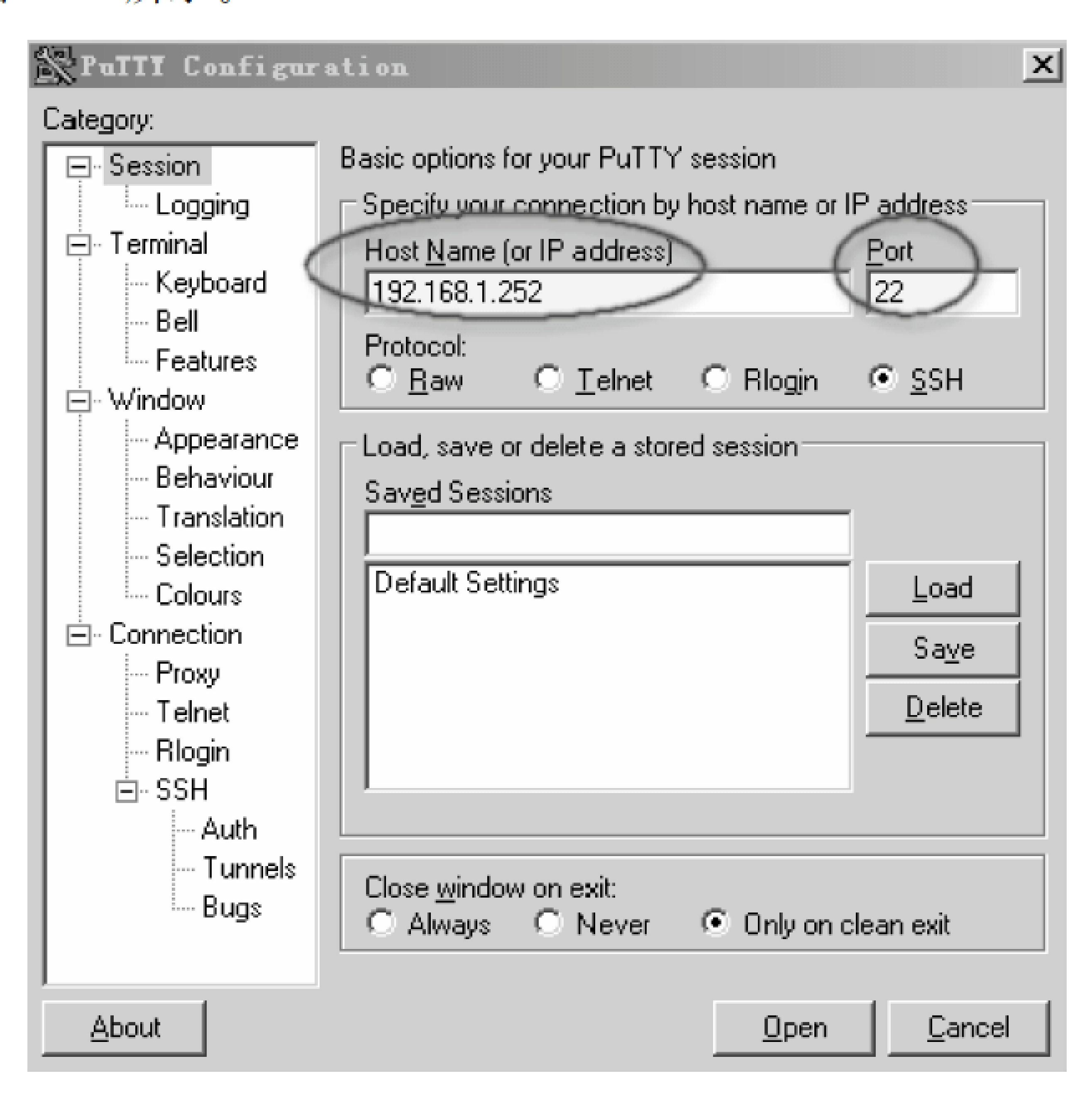


图 2.21　PuTTY 设定

（3）在系统提示后，账户名和密码均为“gengshang”。

（4）打开抓包工具 Wireshark，在过滤框中输入 ssh 过滤 ssh 包，输出如图 2.22 所示的抓包信息。

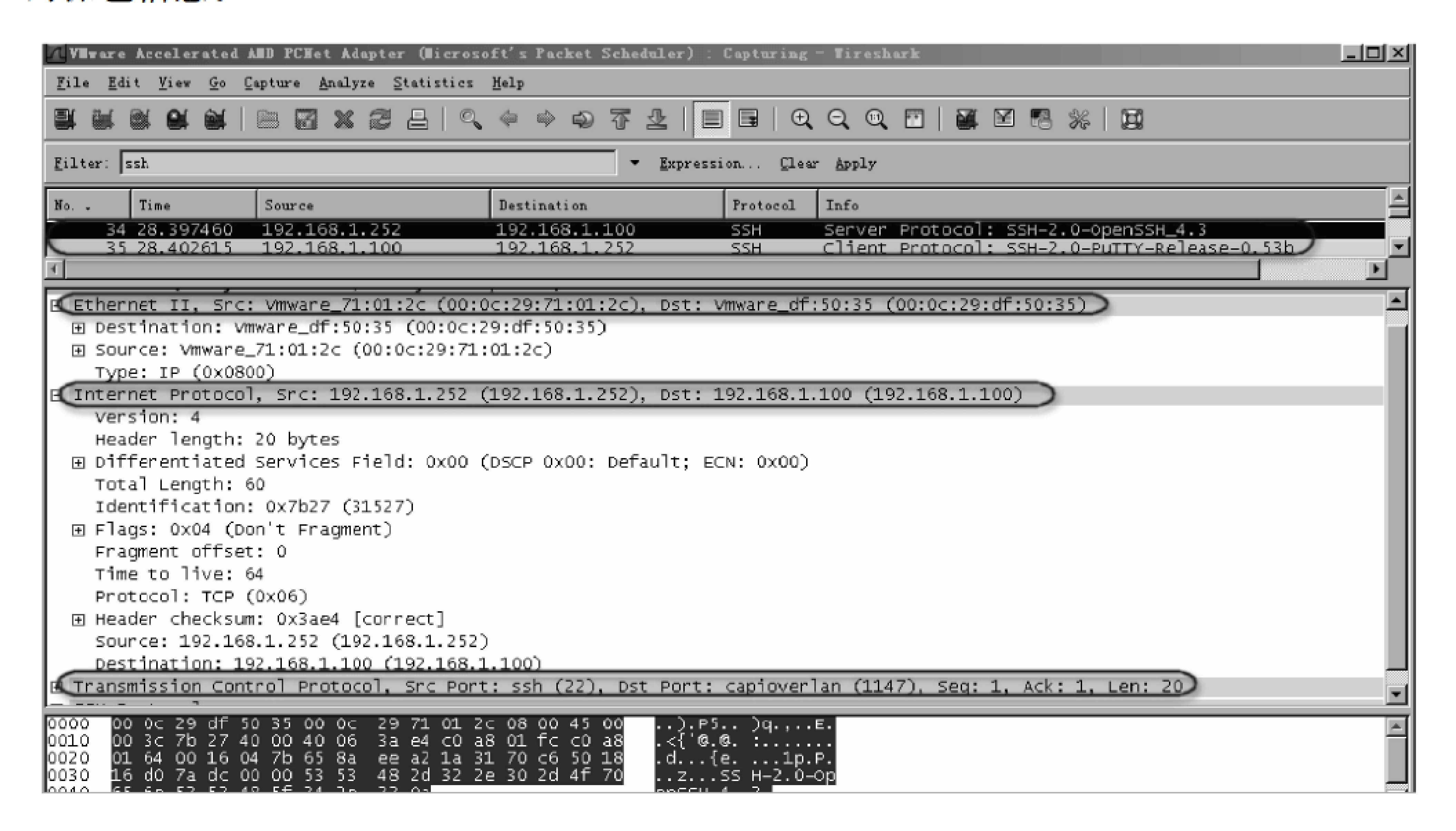


图 2.22　抓包信息

（5）从图 2.23 中看到 ssh 的请求和响应报文，现在抓取 http 报文结合分析整个 ssh 包的第二和第三层信息如下。

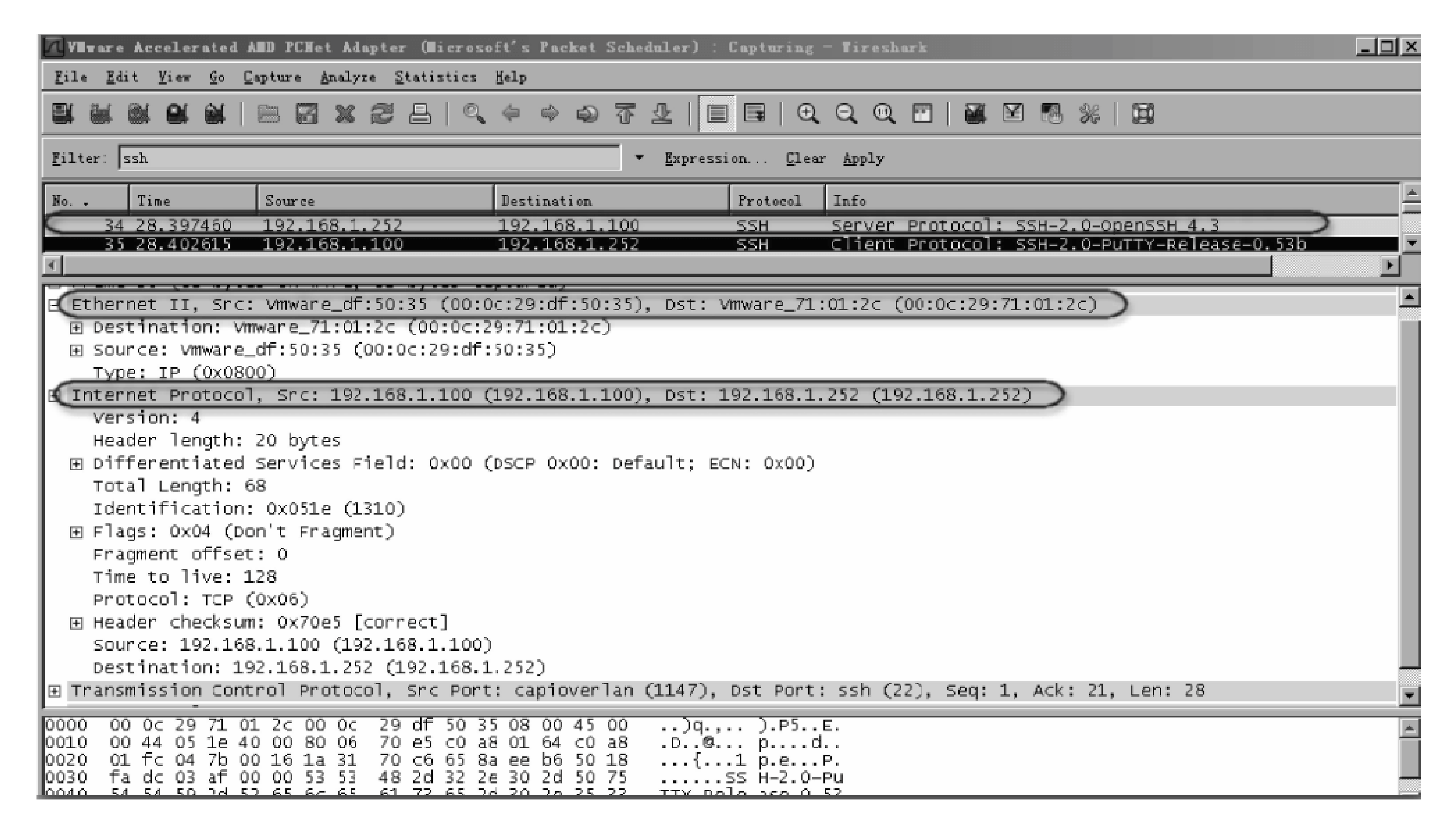


图 2.23　ssh 的请求和响应报文

二层参数：在列表 Ethernet II 部分，指示底层的环境是以太网，协议包中 Ethernet II 型参数给出本机和测试目标主机的二层地址，即 MAC 地址。因为 http get 包是从本地 PC 发给测试目标 PC 的，所以这里的 Src(源 MAC 地址)就是本机网卡的 MAC 地址，在本实验中是 00：0C：29：df：50：35，而 Dst(目标 MAC 地址)在本实验环境下也就是服务器的 MAC 地址。

本实验在纯二层完成，但是如果本地主机和目标测试主机处于三层环境时，这里的 DestinationMAC 就不是目标测试主机的 MAC 地址了，而是本地主机从属网段网关的 MAC 地址。

三层参数：在列表 Internet Protocol 部分，给出测试 ssh 包的源 IPv4 地址和目标 IPv4 地址，其中源 IP 地址(本地主机)为 192.168.1.100；目标 IP 地址(测试主机的 IP 地址)为 192.168.1.252。

(6) 选择 Analyze→Follow TCP Stream 选项，在打开的窗口中显示报文信息，如图 2.24 所示。



图 2.24 ssh 的请求和响应报文分析

从图 2.24 中可分析得到 ssh 对服务进行登录后，账户和密码都经过加密，密文显示因此无法对直接通过抓包分析获得。

4. 思考题

(1) 如何通过 Wireshark 抓取无线包，若有条件可以尝试。

（2）完成跨网段情况下ICMP的请求和响应报文分析，并给出结论。

（3）两台相邻的PC为一个协作小组，一台PC构建FTP服务器使之可以被访问，完成对FTP流量的检测和分析，注意FTP流量和HTTP流量的区别，虽然都为TCP协议，但是FTP使用的两个端口20和21，请指出两个端口的作用，并分析其传输命令如何传输。

（4）分别设计实验内容，完成实验报告。

第3章

病　毒　篇

3.1 引言

编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码被称为计算机病毒(Computer Virus)。病毒具有破坏性、复制性和传染性。

病毒往往会利用计算机操作系统的弱点进行传播，提高系统的安全性是防病毒的一个重要方面，但完美的系统是不存在的，过于强调提高系统的安全性将使系统多数时间用于病毒检查，系统失去了可用性、实用性和易用性，另一方面，信息保密的要求让人们在泄密和抓住病毒之间无法选择。病毒与反病毒将作为一种技术对抗长期存在，两种技术都将随计算机技术的发展而得到长期的发展。

3.2 计算机病毒的概念

计算机病毒在《中华人民共和国计算机信息系统安全保护条例》中被明确定义，病毒指“编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。与生物病毒不同的是几乎所有的计算机病毒都是人为故意制造出来的，有时一旦扩散出来后连编者自己也无法控制。它已经不是一个简单的纯计算机学术问题，而是一个严重的社会问题了。

宏病毒是一种寄存在文档或模板的宏中的计算机病毒，一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。从此以后，所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到其他计算机上。宏病毒具有传播速度极快、制作、变种

方便、破坏可能性极大、多平台交叉感染。

3.3 计算机病毒的产生

病毒不是来源于突发或偶然的原因,一次突发的停电或偶然的错误,会在计算机的磁盘和内存中产生一些乱码和随机指令,但这些代码是无序和混乱的。病毒则是一种比较完美的、精巧严谨的代码,按照严格的秩序组织起来,与所在的系统网络环境相适应和配合。病毒不会通过偶然形成,并且需要有一定的长度,这个基本的长度从概率上来讲是不可能通过随机代码产生的。现在流行的病毒是由人为故意编写的,多数病毒可以找到作者和产地信息,从大量的统计分析来看,病毒作者的主要情况和目的是:一些天才的程序员为了表现自己和证明自己的能力,为了得到控制口令,为了防止编写软件拿不到报酬预留的陷阱等;当然也有因政治、军事、宗教、民族、专利等方面的需求而专门编写的,其中也包括一些病毒研究机构和黑客的测试病毒。

3.4 计算机病毒的传染途径

计算机病毒之所以称为病毒是因为其具有传染性的本质。传统渠道通常有以下几种:

(1) 通过 U 盘。通过使用外界被感染的软盘,例如,不同渠道来的系统盘、来历不明的软件、游戏盘等是最普遍的传染途径。

(2) 通过硬盘。通过硬盘传染也是重要的渠道,由于带有病毒的机器移到其他地方使用、维修等,将干净的软盘传染并再扩散。

(3) 通过网络。这种传染扩散极快,能在很短时间内传遍网络上的机器。

3.5 计算机病毒的特点

1. 寄生性

计算机病毒寄生在其他程序之中,当执行这个程序时,病毒就起破坏作用,而在未启动这个程序之前,它是不易被人发觉的。

2. 传染性

计算机病毒不但本身具有破坏性,更有害的是具有传染性,一旦病毒被复制或产生变种,其速度之快令人难以预防。传染性是病毒的基本特征。在生物界,病毒通过传染从一个生物体扩散到另一个生物体。在适当的条件下,它可得到大量繁殖,使被感染的生物体表现出病症甚至死亡。同样,计算机病毒也会通过各种渠道从已被感染的计算机扩散到未被感染的计算机,是否具有传染性是判别一个程序为计算机病毒的最重要条件。病毒程序通过修改磁盘扇区信息或文件内容,并把自身嵌入到其中的方法达到病毒

的传染和扩散。被嵌入的程序称为宿主程序。

3. 潜伏性

有些病毒像定时炸弹一样,让它什么时间发作是预先设计好的。例如,黑色星期五病毒,不到预定时间一点都觉察不出来,等到条件具备的时候一下子就爆炸开来,对系统进行破坏。一个编制精巧的计算机病毒程序,进入系统之后一般不会马上发作,可以在几周或者几个月内甚至几年内隐藏在合法文件中,对其他系统进行传染,而不被人发现,潜伏性越好,其在系统中的存在时间就会越长,病毒的传染范围就会越大。潜伏性的第一种表现是指病毒程序不用专用检测程序是检查不出来的,因此病毒可以静静地躲在磁盘或磁带里呆上几天,甚至几年,一旦时机成熟,得到运行机会,就要四处繁殖、扩散,继续为害。潜伏性的第二种表现是指计算机病毒的内部往往有一种触发机制,不满足触发条件时,计算机病毒除了传染外不做什么破坏。触发条件一旦得到满足,有的在屏幕上显示信息、图形或特殊标识,有的则执行破坏系统的操作,如格式化磁盘、删除磁盘文件、对数据文件做加密、封锁键盘以及使系统死锁等。

4. 隐蔽性

计算机病毒具有很强的隐蔽性,有的可以通过病毒软件检查出来,有的根本就查不出来,有的时隐时现、变化无常,这类病毒处理起来通常很困难。

5. 破坏性

计算机中毒后,可能会导致正常的程序无法运行,把计算机内的文件删除或受到不同程度的损坏。

6. 可触发性

病毒因某个事件或数值的出现,诱使病毒实施感染或进行攻击的特性称为可触发性。为了隐蔽自己,病毒必须潜伏,少做动作。如果完全不动,一直潜伏的话,病毒既不能感染也不能进行破坏,便失去了杀伤力。病毒既要隐蔽又要维持杀伤力,它必须具有可触发性。病毒的触发机制就是用来控制感染和破坏动作的频率的。病毒具有预定的触发条件,这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时,触发机制检查预定条件是否满足,如果满足,启动感染或破坏动作,使病毒进行感染或攻击;如果不满足,使病毒继续潜伏。

3.6　计算机病毒的分类

根据对计算机病毒的研究,按照科学的、系统的、严密的方法,计算机病毒可以根据以下的属性进行分类。

1. 按照计算机病毒存在的媒体进行分类

根据病毒存在的媒体,病毒可以划分为网络病毒、文件病毒和引导型病毒。网络病毒通过计算机网络传播感染网络中的可执行文件,文件病毒感染计算机中的文件(如

COM、EXE、DOC 等),引导型病毒感染启动扇区(Boot)和硬盘的系统引导扇区(MBR)。还有这三种情况的混合型,例如:多型病毒(文件和引导型)感染文件和引导扇区两种目标,这样的病毒通常都具有复杂的算法,它们使用非常规的办法侵入系统,同时使用了加密和变形算法。

2. 按照计算机病毒传染的方法进行分类

根据病毒传染的方法可分为驻留型病毒和非驻留型病毒。驻留型病毒感染计算机后,把自身的内存驻留部分放在内存(RAM)中,这一部分程序挂接系统调用并合并到操作系统中,它处于激活状态,一直到关机或重新启动。非驻留型病毒在得到机会激活时并不感染计算机内存,一些病毒在内存中留有小部分,但是并不通过这一部分进行传染,这类病毒也被划分为非驻留型病毒。

3. 按照病毒破坏能力划分

根据病毒破坏能力可分为无害型、无危险型、危险型和非常危险型病毒。

(1) 无害型:除了传染时减少磁盘的可用空间外,对系统没有其他影响。

(2) 无危险型:这类病毒仅仅是减少内存、显示图像、发出声音及同类音响。

(3) 危险型:这类病毒在计算机系统操作中造成严重的错误。

(4) 非常危险型:这类病毒删除程序、破坏数据、清除系统内存区和操作系统中重要的信息。

这些病毒对系统造成的危害,并不是本身的算法中存在危险的调用,而是当它们传染时会引起无法预料的、灾难性的破坏。由病毒引起其他的程序产生的错误也会破坏文件和扇区,这些病毒也按照它们引起的破坏能力划分。一些现在的无害型病毒也可能会对新版的 DOS、Windows 和其他操作系统造成破坏。例如,在早期的病毒中,有一个"Denzuk"病毒在 360K 磁盘上很好的工作,不会造成任何破坏,但是在后来的高密度软盘上却能引起大量的数据丢失。

4. 按照病毒特有的算法划分

根据病毒特有的算法可分为伴随型病毒、"蠕虫"型病毒和寄生型病毒。

(1) 伴随型病毒:这一类病毒并不改变文件本身,它们根据算法产生 EXE 文件的伴随体,具有同样的名字和不同的扩展名(COM),例如,XCOPY. EXE 的伴随体是 XCOPY. COM。病毒把自身写入 COM 文件并不改变 EXE 文件,当 DOS 加载文件时,伴随体优先被执行再由伴随体加载执行原来的 EXE 文件。

(2) "蠕虫"型病毒:通过计算机网络传播,不改变文件和资料信息,利用网络从一台机器的内存传播到其他机器的内存,计算网络地址,将自身的病毒通过网络发送。有时它们在系统中存在,一般除了内存不占用其他资源。

(3) 寄生型病毒:除了伴随型和"蠕虫"型病毒,其他病毒均可称为寄生型病毒,它们依附在系统的引导扇区或文件中,通过系统的功能进行传播,按其算法不同又可分为练习型病毒、诡秘型病毒和变型病毒。

练习型病毒:病毒自身包含错误,不能进行很好地传播,例如,一些病毒在调试阶段。

诡秘型病毒：它们一般不直接修改 DOS 中断和扇区数据，而是通过设备技术和文件缓冲区等 DOS 内部修改，不易看到资源，使用比较高级的技术。利用 DOS 空闲的数据区进行工作。

变型病毒（又称幽灵病毒）：这一类病毒使用一个复杂的算法，使自己每传播一份都具有不同的内容和长度。它们一般是由一段混有无关指令的解码算法和被变化过的病毒体组成。

5. 计算机病毒的危害性

计算机资源的损失和破坏，不但会造成资源和财富的巨大浪费，而且有可能造成社会性的灾难，随着信息化社会的发展，计算机病毒的威胁日益严重，反病毒的任务也更加艰巨了。1988 年 11 月 2 日下午 5 时 1 分 59 秒，美国康奈尔大学的计算机科学系研究生，23 岁的莫里斯（Morris）将其编写的蠕虫程序输入计算机网络，致使这个拥有数万台计算机的网络被堵塞。这件事就像是计算机界的一次大地震，引起了巨大反响，震惊全世界，引起了人们对计算机病毒的恐慌，也使更多的计算机专家重视和致力于计算机病毒研究。1988 年下半年，我国在统计局系统首次发现了“小球”病毒，它对统计局系统影响极大，此后由计算机病毒发作而引起的“病毒事件”接连不断，之后发现的 CIH、美丽杀等病毒更是给社会造成了很大损失。

3.7　中毒的诊断

（1）按 Ctrl＋Shift＋Esc 键，调出 Windows 任务管理器查看系统运行的进程，找出不熟悉的进程并记下其名称（这需要经验），如果这些进程是病毒的话，以便于后面的清除。暂时不要结束这些进程，因为有的病毒或非法的进程可能在此没法结束。单击性能查看 CPU 和内存的当前状态，如果 CPU 的利用率接近 100％或内存的占用值居高不下，此时计算机中毒的可能性是 95％。

（2）查看 Windows 当前启动的服务项，执行“开始”→“控制面板”→“管理工具”→“服务”命令，在打开的“服务”窗口中查看右栏状态为“启动”、启动类别为“自动”项的行。一般而言，正常的 Windows 服务，基本上是有描述内容的（少数被黑客或蠕虫病毒伪造的除外），此时双击打开认为有问题的服务项查看其属性中的可执行文件的路径和名称，假如其名称和路径为 C:\winnt\system32\explored.exe，计算机中毒。另一种情况是“控制面板”打不开或者是所有里面的图标跑到左边，中间有一纵向的滚动条，而右边为空白，再双击添加/删除程序或管理工具，窗体内是空的，这是病毒文件 winhlpp32.exe 发作的特性。

（3）运行注册表编辑器，命令为 regedit 或 regedt32，查看都有哪些程序与 Windows 操作系统一起启动。主要查看 Hkey_Local_Machine\Software\microsoft\Windows\CurrentVersion\Run 和后面几个 RunOnce 等，查看窗体右侧的项值，查看是否有非法的启动项。Windows XP 运行 msconfig 也起相同的作用。随着经验的积累，可以轻易地判

断病毒的启动项。

（4）用浏览器上网判断。以前发作的 Gaobot 病毒，可以上 yahoo. com、sony. com 等网站，但是不能访问诸如 www. symantec. com、www. ca. com 这样著名的安全厂商的网站，安装的杀毒软件不能上网升级。

（5）取消隐藏属性，查看系统文件夹 winnt(windows)\system32，如果打开后文件夹为空，表明计算机已经中毒；打开 system32 后，可以对图标按类型排序，查看有没有流行病毒的执行文件存在。顺便查一下文件夹 Tasks、wins、drivers。有的病毒执行文件就藏身于此；drivers\etc 下的文件 hosts 是病毒喜欢篡改的对象，它本来只有 700B 左右，被篡改后就成了 1KB 以上，这是造成一般网站能访问而安全厂商网站不能访问、著名杀毒软件不能升级的原因所在。

（6）由杀毒软件判断是否中毒，如果中毒，杀毒软件会被病毒程序自动终止，并且手动升级失败。

3.8 病毒预防

要预防计算机网络病毒，首先是不要随便从小的个人网站上下载软件。下载软件要到知名度高、信誉良好的站点，通常这些站点软件比较安全。其次不要过于相信和随便运行别人给的软件。要经常检查自己的系统文件，注册表、端口等，多注意安全方面的信息，再次就是修改 Windows 关于隐藏文件扩展名的默认设置，这样可以看清楚文件真正的扩展名。当前许多反病毒软件都具有查杀“木马”或“后门”程序的功能，但仍需更新和采用先进的防病毒软件。最后要提醒的是：如果突然发现自己的计算机硬盘莫名其妙的工作，或者在没有打开任何连接的情况下 Modem 还在“眨眼睛”就立刻断开网络连接，进行木马的搜索。邮件病毒主要通过电子邮件进行传染的，而且大多通过附件夹带，了解了这一点，对于该类病毒的防范就比较明确和容易，要想预防计算机网络病毒，还要做到以下几点。

（1）不要轻易打开陌生人来信中的附件，尤其是一些. EXE 类的可执行文件。

（2）对于比较熟悉的朋友发来的邮件，如果其信中带有附件却未在正文中说明，也不要轻易打开附件，因为它的系统也许已经感染病毒。

（3）不要盲目转发邮件。给别人发送程序文件甚至电子贺卡时，可先在自己的计算机中试一试，确认没有问题后再发，以免无意中成为病毒的传播者。

（4）如果收到主题为“I LOVE YOU”的邮件后立即删除，更不要打开附件。

（5）随时注意反病毒警报，及时更新杀毒软件的病毒代码库。从技术手段上，可安装具有监测邮件系统的反病毒实时监控程序，随时监测系统行为，如使用最新版本的杀毒实时软件来查杀该附件中的文件。切记要注意一点，预防与消除病毒是一项长期的工作任务，不是一劳永逸的，应坚持不懈。

3.9　计算机病毒的清除

计算机病毒的清除,最常用的是杀毒软件。国产杀毒软件主要有瑞星、江民、金山毒霸等;国外杀毒软件有 Kaspersky、PC-Cillion、Norton、McAfee 等。至于哪种杀毒软件最好,或者说更好,众说纷纭。但是,不管选择哪种杀毒软件,一定要使用正版的杀毒软件,切记不要使用盗版杀毒软件。如果计算机有疑似感染病毒的症状时,可以采取如下应急措施。

(1) 将杀毒软件升级至最新版,进行全盘杀毒。最好使用自动升级功能在线升级,如果不能自动升级,也可以下载最新的升级包,进行离线升级。

(2) 如果杀毒软件不能清除病毒,或者重新启动计算机后病毒再次出现。则应该进入安全模式进行查杀。进入安全模式的方法是:在计算机启动自检时按 F8 键,会出现各种启动模式的选择菜单,选择“安全模式”选项即可。

(3) 有些病毒造成杀毒软件无法启动,则需要根据现象,判断病毒的种类,使用相应的专杀工具进行查杀。因为这类病毒虽然能自动关闭杀毒软件,但一般不会关闭专杀工具。使用专杀工具查杀后,升级或重装杀毒软件,再按上面所述的方法进行杀毒。

(4) 如果病毒非常顽固,使用多种方法都不能彻底查杀,则最好格式化并重装操作系统。但是在重装操作系统后,切记不能直接打开除 C 盘外的其他盘,否则病毒又会被激活。必须先做好防护措施,安装杀毒软件,并升级至最新版,对所有硬盘进行杀毒。在确保没有病毒的情况下再打开其他盘。

(5) 有个别病毒在重装操作系统后仍无法彻底清除,则只好对硬盘进行重新分区或进行格式化处理。

实验 5　病毒清除

一、实验目的

了解什么是病毒危害性,了解病毒破坏系统方式,学会简单的清除病毒。

二、实验原理

计算机病毒是一种恶意计算机代码,可以破坏系统程序,占用空间,盗取账号和密码。严重可以导致网络、系统瘫痪。

清除方法:使用安全的杀毒软件清除或了解其原理通过手工清除。

通过 Windows 任务管理器等各种系统自带程序进行疑点排查,逐一清除病毒。

找出病毒真实路径,进行查杀。

三、实验内容

1. 实验环境

(1) 硬件设备:计算机两台 PC-A、PC-B。

(2) 软件工具：冰河木马控制端；文件夹 EXE 病毒。

2. 实验角色

单人操作或双人合作。

3. 实验步骤

1) 冰河木马

本实验将终端 PC-A 作为远程控制攻击端，PC-B 作为受控端进行试验。

(1) 在终端 PC-B 上，打开 Windows 任务管理器，结果如图 3.1 所示。



图 3.1　Windows 任务管理器的初始状态

(2) 在 PC-B 上运行 G_server.exe，再次打开 Windows 任务管理器，结果如图 3.2 所示。



图 3.2　运行 G_server.exe 后 Windows 任务管理器的状态

提示：

实际环境中可以通过邮件、链接等方式将被控制端木马注入到被控制端。这个程序需要在被控制端引诱运行。通常是做成美丽的图片作为伪装，或是通过 QQ 发送，使其运行等。

(3) 在安装 G_server. exe 之前，查看 PC-B 中的资源管理器的进程和性能的运行情况。

(4) 在 PC-A，打开控制端程序：G_CLIENT. EXE，如图 3.3 所示。

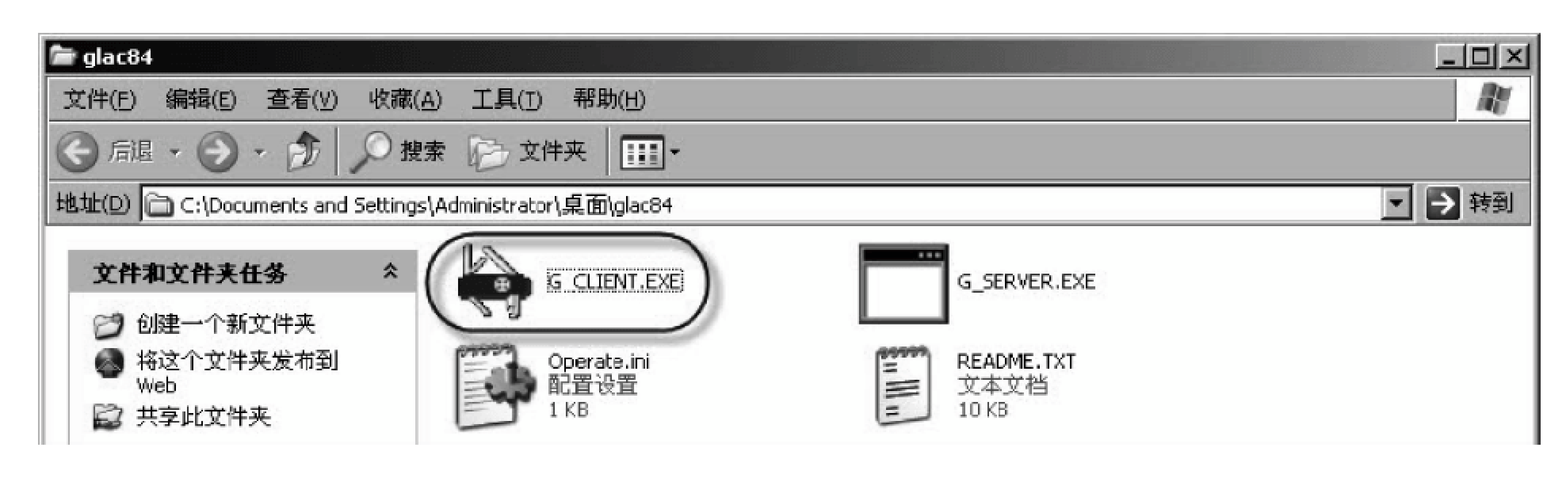


图 3.3 运行 G_CLIENT. EXE

(5) 在冰河主窗口下，单击“添加计算机”图标，如图 3.4 所示。

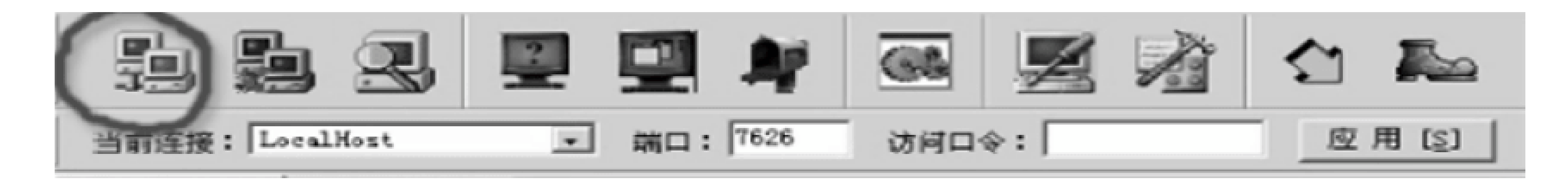


图 3.4 添加计算机

(6) 在显示名称中输入 PC-B 的 IP 地址(本实验中为 192.168.1.20)。

提示：

一般地如果网内有多台设备被植入程序，可以用扫描工具扩大扫描范围，以获取所有的被控主机。

(7) 单击终端 PC-A 冰河主窗口下的“冰河信使”图标，输入任何内容(本实验中为冰河测试)，单击“发送”按钮，如图 3.5 所示，在 PC-B 端，弹出“冰河信使”窗口。这样在 PC-B 和 PC-A 间就建立起了通信。

(8) 在 PC-B 上，将看到接收到的“冰河信使”窗口。

(9) 现在回到被攻击方——机架服务器 Windows 系统，打开 Windows 任务管理器，找到 kernel32. exe 进程，关闭该进程。这个进程就是受控的守护程序，通过它的隐藏，使系统常常被黑客随意联入控制。

(10) 回到控制端，重新扫描，发现已经无法扫描成功，完成破解攻击，如图 3.6 所示。

2) 蠕虫病毒

(1) 插入 U 盘，格式化，并在根目录下新建 3～4 个空文件夹，并退出 U 盘。

(2) 解压桌面上的病毒样本(Recycled. rar)，并运行。

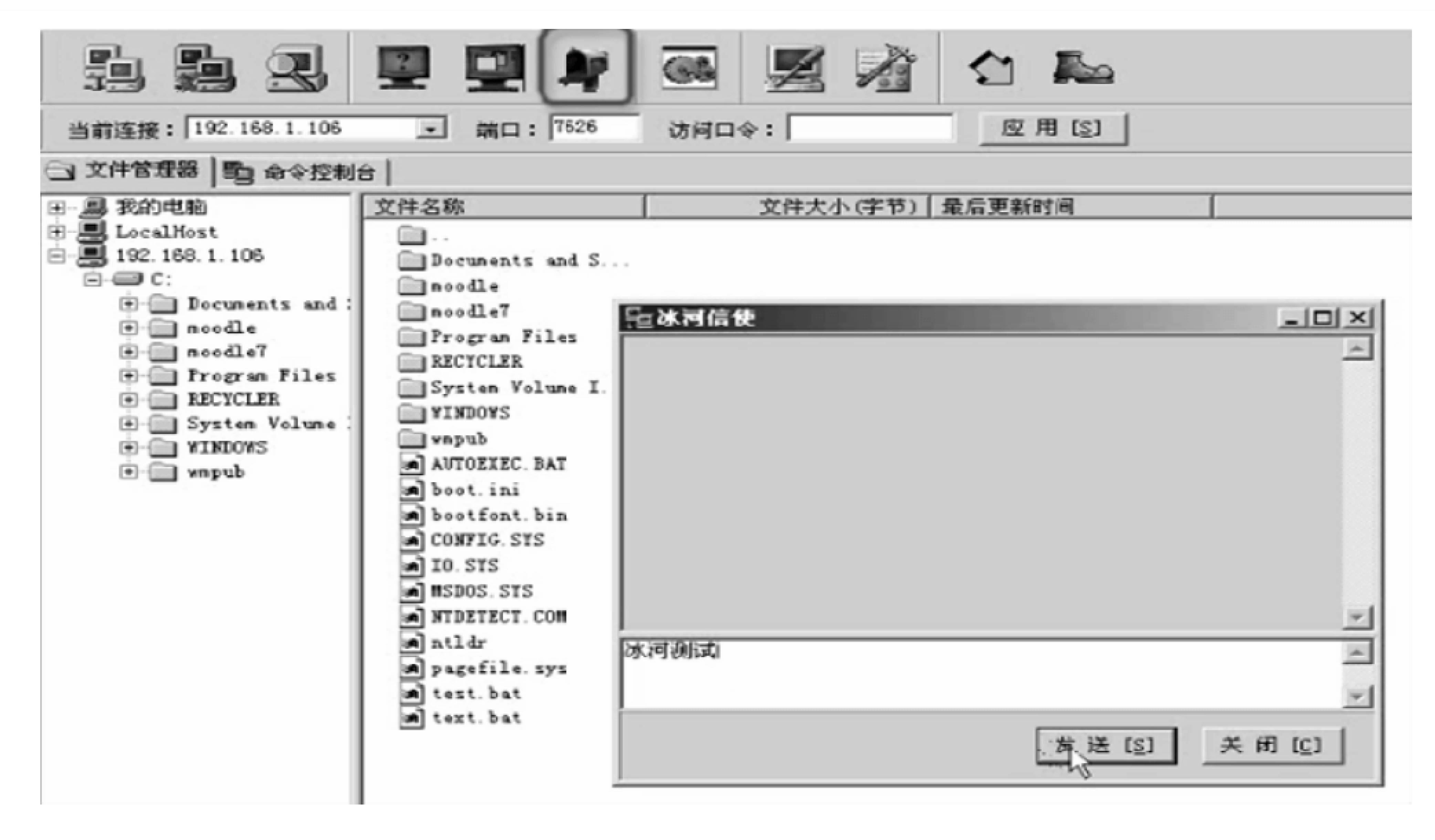


图 3.5 启动冰河信使



图 3.6 扫描失败

(3) 插入 U 盘，并双击 U 盘图标进入，一切看似正常，但右击查看其属性，发现这并不是空文件夹，如图 3.7 所示。



图 3.7　文件夹属性

(4) 选择"工具"→"文件夹选项"选项，然后在"文件夹选项"对话框的"查看"选项卡中去掉隐藏已知扩展名，显示隐藏文件夹和显示隐藏系统文件。

(5) 回到 U 盘查看，发现问题了，U 盘中多了 autorun.inf 文件和文件夹一样的图标却是以.exe 结尾的文件，如图 3.8 所示。真实的文件夹被隐藏，试图取消 Recycle.exe 的隐藏属性却不成功。

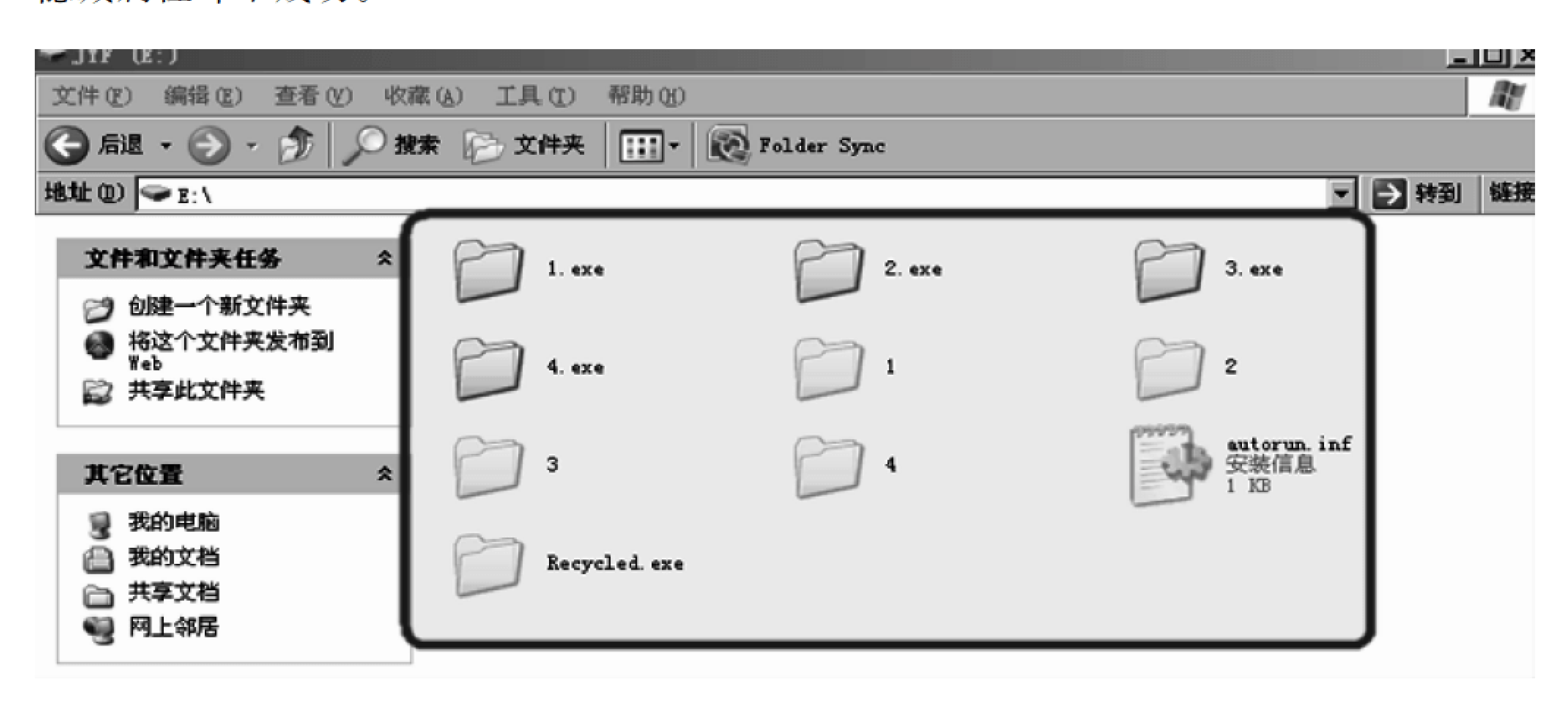


图 3.8　U 盘中的隐藏信息

(6) 把 U 盘中 autorun.inf 的只读属性去掉，用记事本程序打开，发现无论双击还是右击打开 U 盘，自动播放都先指向名为“Recycle.exe”的病毒文件，如图 3.9 所示。

(7) 我们可以做一个实验，把 autorun.inf 中 Recycle.exe 的部分换成 abc.bat。

U 盘根目录新建记事本文件，输入以下代码：

```
@echo off
Echo hellow
pause
```

保存后重命名文件为 abc.bat。

退出 U 盘，再插入计算机中，双击 U 盘盘符，abc.bat 被先打开了，如图 3.10 所示。



图 3.9 autorun.inf



图 3.10 执行 abc.bat

如果那是病毒的话且在其他计算机中，等于是在传播病毒。

autorun.inf 并不是病毒的代名词，是一个自动运行的文件，原来是用来美化与优化用的，而病毒就是利用了这一点，使 U 盘传播病毒。

(8) 开始手动清除病毒。执行“开始”→“运行”命令，在打开的“运行”对话框中输入 cmd，打开命令提示符。

输入：“X：”回车，先定位到你的 U 盘根目录下(X 为你的 U 盘盘符)。

输入：“attrib/s/d-h-s”回车，来清除 U 盘中所有的系统属性和隐藏属性，如图 3.11 所示。

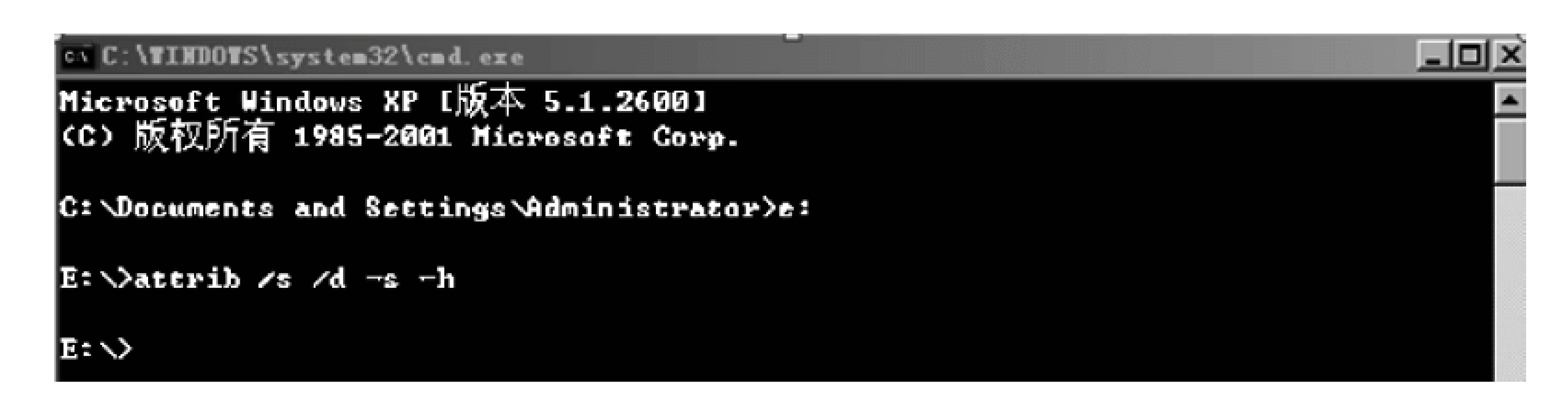


图 3.11 执行 attrib/s/d-h-s

(9) 双击“我的电脑”图标，在地址栏输入“X：”，避免再次触发病毒进入 U 盘，删除 autorun.inf 和一些有着文件夹外表的却以.exe 结尾的病毒，如有 Recycle.exe 一起删除。

(10) 病毒运行时会在 C:\WINDOWS\system32\目录下生成 XP-290F2C69.EXE

文件(后8位随机),找出并删除。可发现删除不掉,说明有程序正在使用,打开任务管理器(按Ctrl+Alt+Delete键)结束可疑进程(与病毒同名),再删除。

4. 思考题

(1) 从网上了解更多关于病毒清除的实验。

(2) 了解一些病毒对注册表的修改。

实验6　网络逻辑炸弹

一、实验目的

通过基于HTML语言的VBScript、JavaScript脚本,学习"逻辑炸弹"的形成、代码形式以及了解危害。

二、实验原理

2002年2月,一名瑞银普惠金融公司的前雇员罗杰·杜罗尼奥(Roger Duronio)因为对公司的奖金发放制度心怀不满,于是在公司网络里安置了一个逻辑炸弹,代码运行后使1000多台计算机丢失重要文件,导致公司股票下跌。这名员工在2006年被判入狱8年。

"逻辑炸弹"是指在特定逻辑条件满足时,实施破坏计算机程序,该程序触发(激活)后造成计算机数据丢失、计算机不能从硬盘或者软盘引导,甚至会使整个系统瘫痪,并出现物理损坏的虚假现象。

"逻辑炸弹"引发时的症状与某些病毒的作用结果相似,并会对社会引发连带性的灾难。与病毒相比,它强调破坏作用本身,而实施破坏的程序不具有传染性。一个"逻辑炸弹"是非常类似的一个真实世界的地雷。

最常见的激活一个逻辑炸弹是一个日期。逻辑炸弹检查系统日期,直到预先编程的日期和时间达成共识,逻辑炸弹被激活并执行它的代码。

因为一个逻辑炸弹不自我复制,这是很容易编写一个逻辑炸弹的计划。这也意味着一个逻辑炸弹将不会蔓延到意想不到的受害者。在某些方面,逻辑炸弹是最文明的程序的威胁,因为一个逻辑炸弹,必须针对特定的受害者。

三、实验内容

1. 实验环境

(1) 硬件设备:小组PC(Windows Server 2003系统)一台。

(2) 软件工具:IE浏览器和写字板编辑软件。

2. 实验步骤

1) 利用JavaScript脚本语言,实现Windows弹出功能。

(1) 新建记事本文件,输入下面的代码。

```
<html><head><title>LoopTest</title>          #标题栏名称
```

```
<metahttp - equiv = "Content - Type"content = "text/html; charset = gb2312">
<scriptlanguage = "JavaScript">                    #进入 JavaScript 语言
functionpop()                                      #定义函数
{for(i = 1; i <= 10; i++)                          #循环出现窗体的次数
{window.open
('http:#www.sohu.com','','width = 400,height = 460','status = off','location = off','toolbar =
off','scrollbars = off')                           #定义打开网页的地址及窗口大小等
}
}
</script>                                          #JavaScript 语言结束
</head><bodybgcolor = "#FFFFFF"text = "#000000">
    #定义窗体背景色等颜色 FFFFFF 为黑色,000000 为白色
<formname = "form">
<p>inputtype = "button"value = "一按你就知道了"onClick = "pop()"name = "button"class =
"unnamed1">                                        #创建按钮</p>
</form></body></html>
```

(2) 保存后运行,完成后修改后缀名,把 txt 换成 html。

(3) 双击运行效果如图 3.12 所示。



图 3.12 执行后效果

(4) 使其允许 ActiveX 控件,如图 3.13 所示。



图 3.13 允许 ActiveX 控件

（5）单击“一按你就知道了”按钮，观察效果。搜狐网页以宽 400、高 460 的大小被瞬间打开 10 次，如图 3.14 所示。

如果把 for 循环改成一个死循环，那对系统的破坏性就很可怕。



图 3.14　运行实验程序后的效果

2）炸弹欺骗攻击

（1）新建记事本，重命名为 bomp.txt。

（2）输入下面代码：

```
<HTML>
<scriptlanguage='VBScript'>                       #VBScript 语言开始
DIMbomp#定义 bomp
setbomp=CreateObject("WScript.Shell")             #建立对象
bomp.run("C:\Windows\notepad.exe")                #指定程序运行时打开的文件
                                                  #VBScript 语言结束
</SCRIPT>
</HTML>
```

（3）完成后保存，重命名文件，修改其后缀名为 bomp.html。

（4）双击运行 bomp.html。

（5）允许 ActiveX 控件(同实验 1))。

（6）运行效果，如图 3.15 所示。

（7）还可以让附带打开的程序隐藏，只需在 bomp.run("C:\Windows\notepad.exe")中添加“,vbhide”，即 bomp.run("C:\Windows\notepad.exe"),vbhide，再运行 bomp.html，表面上像无记事本程序打开。

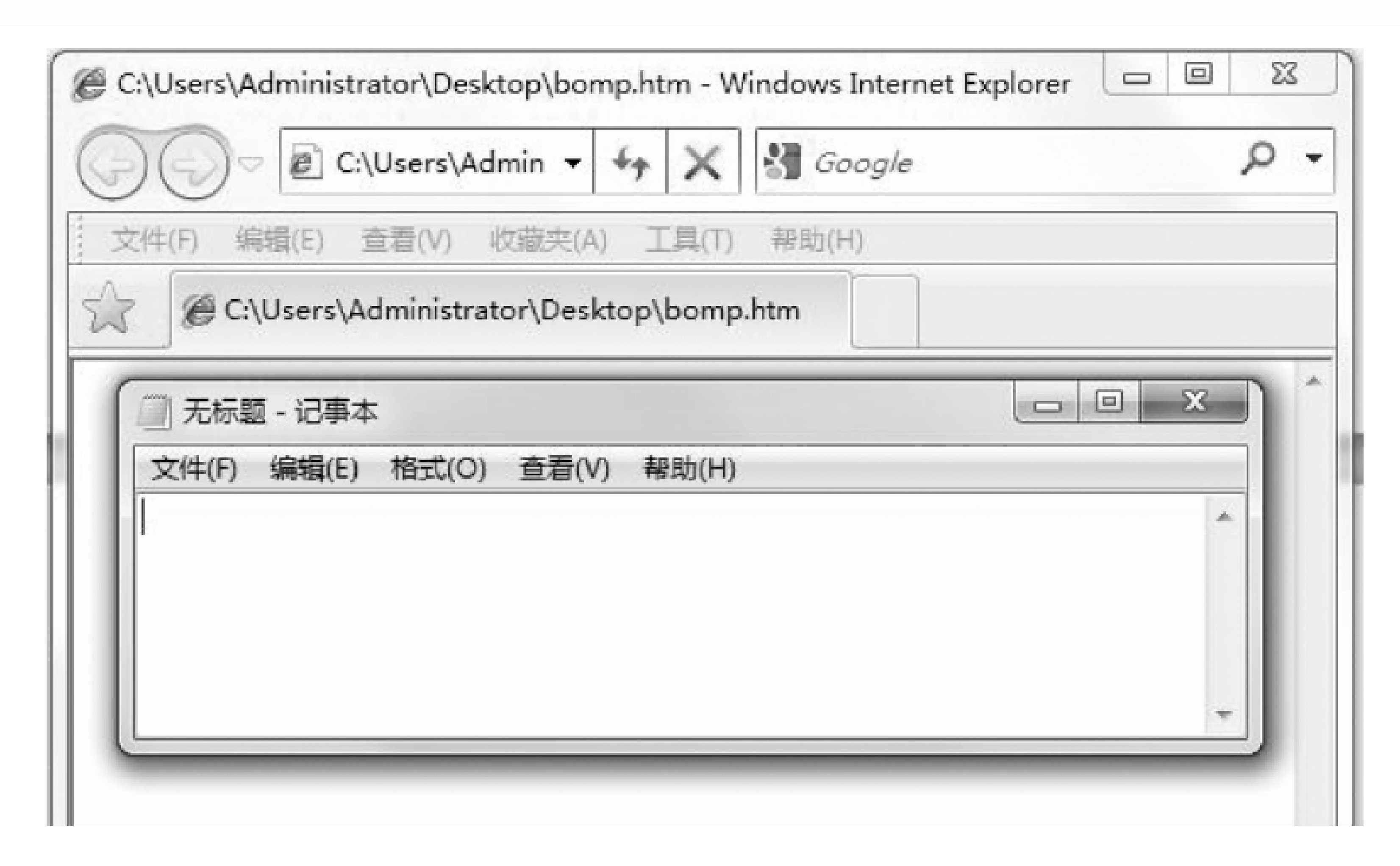


图 3.15 记事本文件被随着网页打开而打开

(8) 再打开 Windows 任务管理器查看，记事本程序其实已经打开，而用户并不知道。在 bomp.run("C:\Windows\notepad.exe")语句中，可以修改成其他文件，比如说是一个已存在计算机中的恶意程序等，此时它的破坏性就非常可怕。

3. 思考题

(1) 尝试编写一些基于 WSH(WindowsScript Host)环境的脚本语言，并使之形成死循环。

(2) 体会浏览器对 ActiveX 控件阻止的重要性以及如何对上网浏览器的恰当设置。

第4章

应用安全篇

4.1 引言

信息和应用安全本身包括的范围很大，大到国家军事政治等机密安全，小范围的当然还包括如防范商业企业机密泄露、防范青少年对不良信息的浏览、个人信息的泄露等。网络环境下的信息和应用安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名、信息认证、数据加密等），直至安全系统，其中任何一个安全漏洞便可以威胁全局安全。

我国的改革开放带来了各方面信息量的急剧增加，并要求大容量、高效率地传输这些信息。为了适应这一形势，通信技术发生了前所未有的爆炸性发展。目前，除有线通信外，短波、超短波、微波、卫星等无线电通信也正在越来越广泛地应用。与此同时，国外敌对势力为了窃取我国的政治、军事、经济、科学技术等方面的秘密信息，运用侦察台、侦察船、卫星等手段，形成固定与移动、远距离与近距离、空中与地面相结合的立体侦察网，截取我国通信传输中的信息。

4.2 Serv-U 搭建 FTP

4.2.1 Serv-U 简介

Serv-U 是一种被广泛运用的 FTP 服务器端软件，支持 3x/9x/ME/NT/2K 等全 Windows 系列。可以设定多个 FTP 服务器、限定登录用户的权限、登录主目录及空间大小等，功能非常完备。它具有非常完备的安全特性，支持 SSL FTP 传输，支持在多个

Serv-U 和 FTP 客户端通过 SSL 加密连接保护数据安全等。

Serv-U 是目前众多的 FTP 服务器软件之一。通过使用 Serv-U，用户能够将任何一台 PC 设置成一个 FTP 服务器，这样，用户或其他使用者就能够使用 FTP 协议，通过在同一网络上的任何一台 PC 与 FTP 服务器连接，进行文件或目录的复制、移动、创建和删除等。这里提到的 FTP 协议是专门被用来规定计算机之间进行文件传输的标准和规则，正是因为有了像 FTP 这样的专门协议，才使得人们能够通过不同类型的计算机，使用不同类型的操作系统，对不同类型的文件进行相互传递。

4.2.2 Serv-U 的原理

Serv-U 由引擎和用户界面两大部分组成。Serv-U 引擎（ServUDaemon.exe）其实是一个常驻后台的程序，也是 Serv-U 整个软件的心脏部分，它负责处理来自各种 FTP 客户端软件的 FTP 命令，也是负责执行各种文件传送的软件。在运行 Serv-U 引擎也就是 ServUDaemon.exe 文件后，我们看不到任何的用户界面，它只是在后台运行，通常我们无法影响它，但在 ServUAdmin.exe 中我们可以停止和开始它。Serv-U 引擎可以在任何 Windows 平台下作为一个本地系统服务来运行，系统服务随操作系统的启动而开始运行，而后我们就可以运行用户界面程序了。Serv-U 用户界面（ServUAdmin.exe）也就是 Serv-U 管理员，它负责与 Serv-U 引擎之间的交互。它可以让用户配置 Serv-U，包括创建域、定义用户并告诉服务器是否可以访问。启动 Serv-U 管理员最简单的办法就是直接单击系统栏的“U”形图标，当然，也可以从“开始”菜单中运行它。

4.2.3 Serv-U 的功能

(1) 符合 Windows 标准的用户界面友好亲切，易于掌握。

(2) 支持实时的多用户连接，支持匿名用户的访问。

(3) 通过限制同一时间最大的用户访问人数确保 PC 的正常运转。

(4) 安全性能出众。在目录和文件层次都可以设置安全防范措施。

(5) 能够为不同用户提供不同设置，支持分组管理数量众多的用户。

(6) 可以基于 IP 对用户授予或拒绝访问权限。

(7) 支持文件上传和下载过程中的断点续传。

(8) 支持拥有多个 IP 地址的多宿主站点。

(9) 能够设置上传和下载的比率、硬盘空间配额、网络使用带宽等，从而能够保证用户有限的资源不被大量的 FTP 访问用户所消耗。

(10) 可作为系统服务后台运行。

(11) 可自用设置在用户登录或退出时的显示信息，支持具有 UNIX 风格的外部链接。

4.3 FTP

4.3.1 FTP 简介

FTP——文件传输协议(File Transfer Protocol)是一个用于在两台装有不同操作系统的机器中传输计算机文件的软件标准。它属于网络协议组的应用层。FTP 是一个 8 位的客户端-服务器协议,能操作任何类型的文件而不需要进一步处理,就像 MIME 或 Unencode 一样。但是,FTP 有着极高的延时,这意味着,从开始请求到第一次接收需求数据之间的时间会非常长。

FTP 服务一般运行在 20 和 21 两个端口。端口 20 用于在客户端和服务器之间传输数据流,而端口 21 用于传输控制流,并且是命令通向 FTP 服务器的进口。当数据通过数据流传输时,控制流处于空闲状态。而当控制流空闲很长时间后,客户端的防火墙会将其会话置为超时,这样当大量数据通过防火墙时,会产生一些问题。此时,虽然文件可以成功的传输,但因为控制会话会被防火墙断开,传输会产生一些错误。

4.3.2 FTP 的功能

FTP 具有以下功能:

(1) 促进文件的共享(计算机程序或数据)。

(2) 鼓励间接或者隐式的使用远程计算机。

(3) 向用户屏蔽不同主机中各种文件存储系统的细节。

(4) 可靠和高效的传输数据。

4.3.3 FTP 的缺点

FTP 具有以下缺点:

(1) 密码和文件内容都使用明文传输,可能产生不希望发生的窃听。

(2) 因为必需开放一个随机的端口以建立连接,当防火墙存在时,客户端很难过滤处于主动模式下的 FTP 流量。

4.3.4 FTP 的应用原理

FTP 也是基于 C/S 模式而设计的。在进行 FTP 操作时,既需要客户应用程序,也需要服务器端程序。我们一般先在自己的计算机中执行 FTP 客户应用程序,在远程服务器中执行 FTP 服务器应用程序,这样,就可以通过 FTP 客户应用程序和 FTP 进行连接。连接成功后,可以进行各种操作。在 FTP 中,客户机只提出请求和接收服务,服务器只接收请求和执行服务。

在利用 FTP 进行文件传输之前,用户必须先联入 Internet 中,在用户自己的计算机上启动 FTP 用户应用程序,并且利用 FTP 应用程序和远程服务器建立连接,激活远程服

务器上的FTP服务器程序。准备就绪后,用户首先向FTP服务器提出文件传输申请,FTP服务器找到用户所申请的文件后,利用TCP/IP将文件的副本传送到用户的计算机上,用户的FTP程序再将接收到的文件写入自己的硬盘。文件传输完成后,用户计算机与服务器计算机的连接自动断开。

与其他的C/S模式不同的是,FTP协议的客户机与服务器之间需要建立双重连接:一个是控制连接;另一个是数据连接。这样,在建立连接时就需要占用两个通信信道。

4.4 匿名FTP

4.4.1 匿名FTP简介

用于对远程计算机的连接,这些计算机是作为匿名或客户用户进行连接的,以将公共文件传输到用户的本地计算机。匿名FTP是这样一种机制:用户可通过它连接到远程主机上,并从其下载文件,而无须成为其注册用户。系统管理员建立了一个特殊的用户ID,名为anonymous,Internet上的任何人在任何地方都可使用该用户ID。通过FTP程序连接匿名FTP主机的方式同连接普通FTP主机的方式差不多,只是在要求提供用户标识ID时必须输入anonymous,该用户ID的口令可以是任意的字符串。

值得注意的是,匿名FTP不适用于所有Internet主机,它只适用于那些提供了这项服务的主机。当远程主机提供匿名FTP服务时,会指定某些目录向公众开放,允许匿名存取,系统中的其余目录则处于隐匿状态。作为一种安全措施,大多数匿名FTP主机都允许用户从其下载文件,而不允许用户向其上传文件,也就是说,用户可将匿名FTP主机上的所有文件全部复制到自己的机器上,但不能将自己机器上的任何一个文件复制至匿名FTP主机上。即使有些匿名FTP主机确实允许用户上传文件,用户也只能将文件上传至某一指定上传目录中。随后,系统管理员会去检查这些文件,他会将这些文件移至另一个公共下载目录中,供其他用户下载。利用这种方式,远程主机的用户得到了保护,避免了有人上传有问题的文件,如带病毒的文件。

4.4.2 匿名FTP的特点

匿名FTP具有以下特点:

(1) 匿名FTP运用很广,没有什么指定的要求。所以,每一个人都可以在匿名FTP主机上访问文件。

(2) 在Internet上,匿名FTP是软件分发的主要方式。在Internet上保存所有已提供所用标准协议的有用程序。许多程序通过匿名FTP分布,每一个人都可以建立一个Internet主机。

4.5 缓冲区溢出程序代码分析

4.5.1 缓冲区溢出简介

缓冲区又称为缓存,是内存空间的一部分。也就是说,在内存空间中预留了一定的存储空间,这些存储空间用来缓冲输入或输出的数据,这部分预留的空间就称为缓冲区。

缓冲区根据其对应的是输入设备还是输出设备,可分为输入缓冲区和输出缓冲区。

4.5.2 缓冲区的作用

缓冲区的作用是为了解决速度不匹配的问题,高速的 CPU 与内存,内存与硬盘,CPU 与 I/O 等速度不匹配的问题,而引入缓冲区,例如,从磁盘里读取信息,先把读出的数据放在缓冲区,计算机再直接从缓冲区中读取数据,等缓冲区的数据读取完后再到磁盘中读取,这样就可以减少磁盘的读写次数,再加上计算机对缓冲区的操作大大快于对磁盘的操作,故应用缓冲区可大大提高计算机的运行速度。缓冲区就是一块内存区,它用在输入/输出设备和 CPU 之间,用来缓存数据。它使得低速的输入/输出设备和高速的 CPU 能够协调工作,避免低速的输入/输出设备占用 CPU。

4.5.3 缓冲区的类型

缓冲区分为三种类型:全缓冲、行缓冲和不带缓冲。

(1) 全缓冲:在这种情况下,当填满标准 I/O 缓存后才进行实际 I/O 操作。全缓冲的典型代表是对磁盘文件的读写。

(2) 行缓冲:在这种情况下,当在输入和输出中遇到换行符时,执行真正的 I/O 操作。这时,用户输入的字符先存放在缓冲区,等按下 Enter 键换行时才进行实际的 I/O 操作。行缓冲的典型代表是键盘输入数据。

(3) 不带缓冲:不带缓冲也就是不进行缓冲,标准出错情况 stderr 是典型代表,这使得出错信息可以直接尽快地显示出来。

4.5.4 缓冲区溢出攻击

缓冲区溢出攻击有多种英文名称:bufferoverflow、bufferoverrun、smashthestack、trashthestack、scribblethestack、manglethestack、memoryleak、overrunscrew,它们是指同一种攻击手段。第一个缓冲区溢出攻击是 Morris 蠕虫,发生在 20 年前,它曾造成了全世界 6000 多台网络服务器瘫痪。

缓冲区溢出是指当计算机向缓冲区内填充数据位数时超过了缓冲区本身的容量溢出的数据覆盖在合法数据上,理想的情况是程序检查数据长度并不允许输入超过缓冲区长度的字符,但是绝大多数程序都会假设数据长度总是与所分配的储存空间相匹配,这就为缓冲区溢出埋下隐患,操作系统所使用的缓冲区又被称为“堆栈”,在各个操作进程

之间，指令会被临时储存在“堆栈”当中，“堆栈”也会出现缓冲区溢出。

注意：堆栈都是一种数据项按序排列的数据结构，只能在一端（称为栈顶（top））对数据项进行插入和删除。

4.5.5 缓冲区溢出的危害

在当前网络与分布式操作系统安全中，被广泛利用的50%以上都是缓冲区溢出，其中最著名的例子是1988年利用fingerd漏洞的蠕虫。而缓冲区溢出中，最为危险的是堆栈溢出，因为入侵者可以利用堆栈溢出，在函数返回时改变返回程序的地址，让其跳转到任意地址，带来的危害一种是程序崩溃导致拒绝服务，另外一种就是跳转并且执行一段恶意代码，例如得到shell，然后为所欲为。

4.5.6 缓冲区溢出的原理

通过往程序的缓冲区写入超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，造成程序崩溃或使程序转而执行其他指令，以达到攻击的目的。造成缓冲区溢出的原因是程序中没有仔细检查用户输入的参数。

4.5.7 缓冲区溢出的攻击

在1998年Lincoln实验室用来评估入侵检测的5种远程攻击中，有2种是缓冲区溢出。而在1998年CERT的13份建议中，有9份是与缓冲区溢出有关的，在1999年，至少有半数的建议是和缓冲区溢出有关的。在Bugtraq的调查中，有2/3的被调查者认为缓冲区溢出漏洞是一个很严重的安全问题。

缓冲区溢出成为远程攻击的主要手段其原因在于缓冲区溢出漏洞给予了攻击者想要的一切：植入并且执行攻击代码。被植入的攻击代码以一定的权限运行有缓冲区溢出漏洞的程序，从而得到被攻击主机的控制权。

为了达到这个目的，攻击者必须达到如下的两个目标：

（1）在程序的地址空间里安排适当的代码。

（2）通过适当的初始化寄存器和内存，让程序跳转到入侵者安排的地址空间执行。

4.5.8 在地址空间里安排适当的代码的方法

1. 植入法

攻击者向被攻击的程序输入一个字符串，程序会把这个字符串放到缓冲区里。这个字符串包含的资料是可以在这个被攻击的硬件平台上运行的指令序列。在这里，攻击者用被攻击程序的缓冲区来存放攻击代码。缓冲区可以设在任何地方：堆栈（stack，自动变量）、堆（heap，动态分配的内存区）和静态资料区。

2. 利用已经存在的代码

有时，攻击者想要的代码已经在被攻击的程序中了，攻击者所要做的只是对代码传

递一些参数。例如，攻击代码要求执行"exec("/bin/sh")"，而在 libc 库中的代码执行"exec(arg)"，其中 arg 是一个指向一个字符串的指针参数，那么攻击者只要把传入的参数指针改向指向"/bin/sh"。

3. 控制程序转移到攻击代码的方法

所有的这些方法都是在寻求改变程序的执行流程，使之跳转到攻击代码。最基本的就是溢出一个没有边界检查或者其他弱点的缓冲区，这样就扰乱了程序的正常的执行顺序。通过溢出一个缓冲区，攻击者可以用暴力的方法改写相邻的程序空间而直接跳过了系统的检查。分类的基准是攻击者所寻求的缓冲区溢出的程序空间类型，原则上是可以任意的空间，实际上，许多的缓冲区溢出是用暴力的方法来寻求改变程序指针的。这类程序的不同之处就是程序空间的突破和内存空间的定位不同。

(1) 活动记录(Activation Records)。每当一个函数调用发生时，调用者会在堆栈中留下一个活动记录，它包含了函数结束时返回的地址。攻击者通过溢出堆栈中的自动变量，使返回地址指向攻击代码。通过改变程序的返回地址，当函数调用结束时，程序就跳转到攻击者设定的地址，而不是原先的地址。这类的缓冲区溢出被称为堆栈溢出攻击(Stack Smashing Attack)，是目前最常用的缓冲区溢出攻击方式。

(2) 函数指针(Function Pointers)。函数指针可以用来定位任何地址空间。例如，"void(* foo)()"声明了一个返回值为 void 的函数指针变量 foo。所以攻击者只需在任何空间内的函数指针附近找到一个能够溢出的缓冲区，然后溢出这个缓冲区来改变函数指针。在某一时刻，当程序通过函数指针调用函数时，程序的流程就按攻击者的意图实现了。它的一个攻击范例就是在 Linux 系统下的 superprobe 程序。

(3) 长跳转缓冲区(Longjmp Buffers)。在 C 语言中包含了一个简单的检验/恢复系统，称为 setjmp/longjmp。意思是在检验点设定"setjmp(buffer)"，用"longjmp(buffer)"来恢复检验点。然而，如果攻击者能够进入缓冲区的空间，那么"longjmp(buffer)"实际上是跳转到攻击者的代码。像函数指针一样，longjmp 缓冲区能够指向任何地方，所以攻击者所要做的就是找到一个可供溢出的缓冲区。一个典型的例子就是 Perl5.003 的缓冲区溢出漏洞；攻击者首先进入用来恢复缓冲区溢出的 longjmp 缓冲区，然后诱导进入恢复模式，这样就使 Perl 的解释器跳转到攻击代码上了。

4.5.9 代码植入和流程控制技术的综合分析

最简单和常见的缓冲区溢出攻击类型就是在一个字符串里综合了代码植入和活动记录技术。攻击者定位一个可供溢出的自动变量，然后向程序传递一个很大的字符串，在引发缓冲区溢出，改变活动记录的同时植入了代码。这是由 Levy 指出的攻击的模板。因为 C 语言在习惯上只为用户和参数开辟很小的缓冲区，因此这种漏洞攻击的实例十分常见。

代码植入和缓冲区溢出不一定要在一次动作内完成。攻击者可以在一个缓冲区内放置代码，这是不能溢出的缓冲区。然后，攻击者通过溢出另外一个缓冲区来转移程序

的指针。这种方法一般用来解决可供溢出的缓冲区不够大(不能放下全部的代码)的情况。如果攻击者试图使用已经常驻的代码而不是从外部植入代码,他们通常必须把代码作为参数调用。举例来说,在 libc(几乎所有的 C 程序都要它来连接)中的部分代码段会执行“exec(something)”,其中 somthing 就是参数。攻击者使用缓冲区溢出改变程序的参数,然后利用另一个缓冲区溢出使程序指针指向 libc 中的特定的代码段。

4.5.10 缓冲区溢出攻击的防范方法

缓冲区溢出攻击占了远程网络攻击的绝大多数,这种攻击可以使得一个匿名的 Internet 用户有机会获得一台主机的部分或全部的控制权。如果能有效地消除缓冲区溢出的漏洞,则很大一部分的安全威胁可以得到缓解。

(1) 通过操作系统使得缓冲区不可执行,从而阻止攻击者植入攻击代码。通过使被攻击程序的数据段地址空间不可执行,从而使得攻击者不可能执行被植入被攻击程序输入缓冲区的代码,这种技术被称为非执行的缓冲区技术。在早期的 UNIX 系统设计中,只允许程序代码在代码段中执行。但是近来的 UNIX 和 MSWindows 系统由于要实现更好的性能和功能,往往在数据段中动态地放入可执行的代码,这也是缓冲区溢出的根源。为了保持程序的兼容性,不可能使得所有程序的数据段不可执行。但是可以设定堆栈数据段不可执行,这样就可以保证程序的兼容性。Linux 和 Solaris 都发布了有关这方面的内核补丁。

(2) 利用编译器的边界检查来实现缓冲区的保护。编写正确的代码是一件非常有意义的工作,特别像编写 C 语言那种风格自由而容易出错的程序,这种风格是由于追求性能而忽视正确性的传统引起的。尽管花了很长的时间使得人们知道了如何编写安全的程序,具有安全漏洞的程序依旧出现。因此,人们开发了一些工具和技术来帮助经验不足的程序员编写安全正确的程序。最简单的方法就是用 grep 来搜索源代码中容易产生漏洞的库的调用,如对 strcpy 和 sprintf 的调用,这两个函数都没有检查输入参数的长度。事实上,各个版本 C 的标准库均有这样的问题存在。此外,人们还开发了一些高级的查错工具,如 faultinjection 等。这些工具的目的在于通过人为随机地产生一些缓冲区溢出来寻找代码的安全漏洞。还有一些静态分析工具用于侦测缓冲区溢出的存在。虽然这些工具帮助程序员开发更安全的程序,但是由于 C 语言的特点,这些工具不可能找出所有的缓冲区溢出漏洞。所以,侦错技术只能用来减少缓冲区溢出的可能,并不能完全地消除它的存在。

实验 7 在 Serv-U 中配置安全的 FTP 服务

一、实验目的

学会常用的 FTP 工具 Serv-U 程序中配置安全的 FTP 服务,从而体验了解安全的 FTP 的要求。

二、实验原理

利用 Serv-U 软件搭建 FTP 服务器，对端口配置、用户控制、用户组设置、权限设置、目录设置等功能进行配置，尤其通过 SSL 加密设置、分析安全的 FTP 设置和不安全的 FTP 设置，通过 FTP 工具 FlashFXP 或其他，对服务器的信息进行获取。

三、实验内容

1. 实验环境

(1) 硬件设备：小组 PC 一台，用于访问 Windows Server 2003 服务器；Windows Server 2003 服务器，用于搭建 FTP 服务器。

(2) 实验工具：Serv-U 软件(绿色版，在服务器上安装成功，登录服务器可以运行)；FlashFXP，从平台上下载，单击 flashfxp.exe 运行就可以；Wireshark，在客户端上已经安装好。

实验拓扑图和实验设备配置信息分别如图 4.1 和表 4.1 所示。

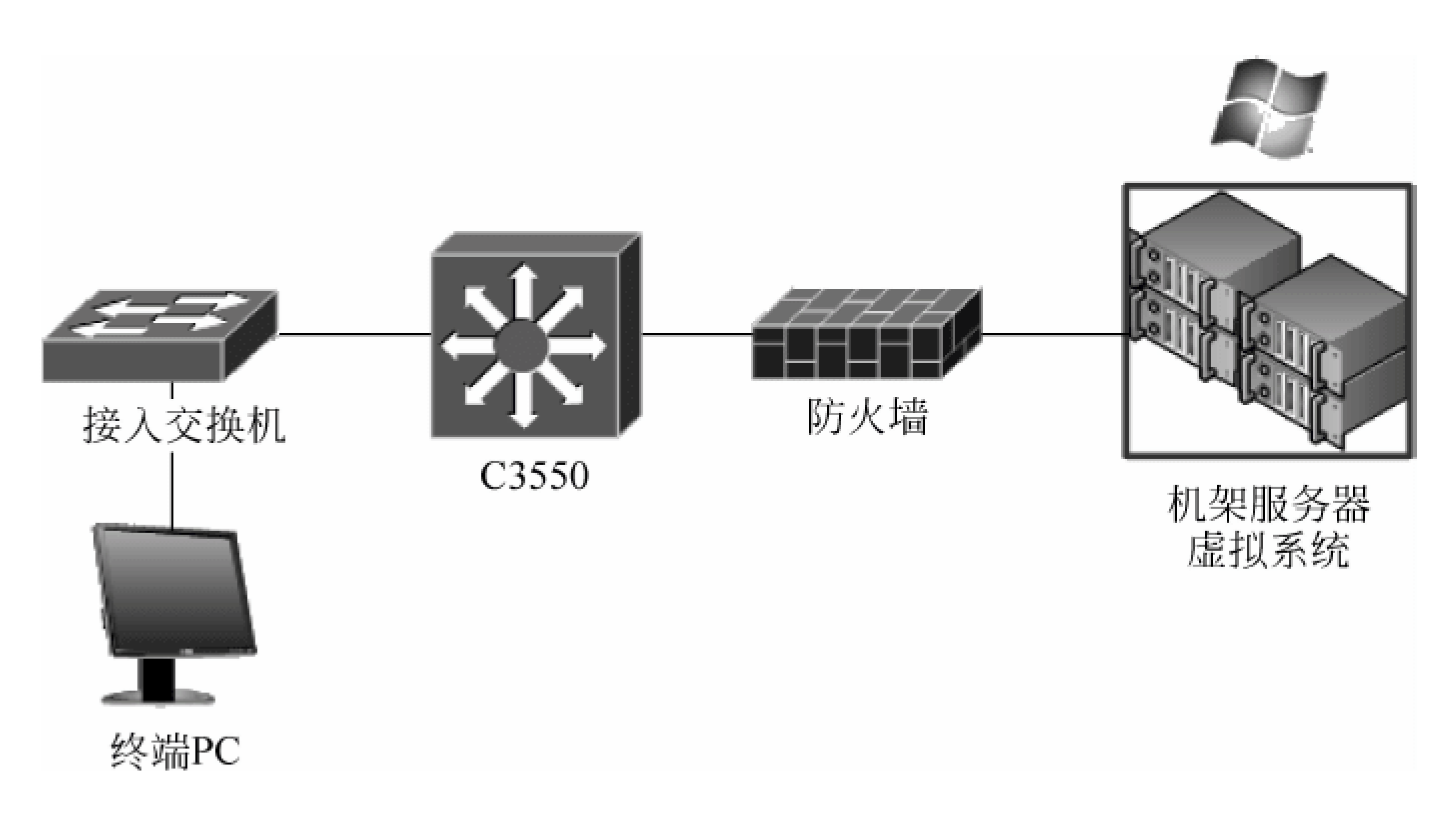


图 4.1　实验拓扑图

表 4.1　实验设备配置参考信息表

设 备 名 称	IP 地址
示例实验终端 PC	192.168.1.188
示例实验 Windows Server 2003 服务器	192.168.1.251

2. 实验步骤

1) 基本设置

(1) 在终端 PC 上，远程登录 Windows Server 2003 服务器。执行开始→运行命令，在打开的“运行”对话框中输入“mstsc”命令，在打开“远程桌面连接”窗口中，输入 IP 地址“192.168.1.251”，密码为“gengshang”。然后双击桌面的 servuadmin.exe，运行 Serv-U 软件，如图 4.2 所示。

(2) 右击“域”，在弹出的快捷菜单中选择“新建域”选项，打开“添加新建域”对话框，输入 IP 地址“192.168.1.251”，如图 4.3 所示，单击“下一步”按钮。



图 4.2 启动 Serv-U 软件

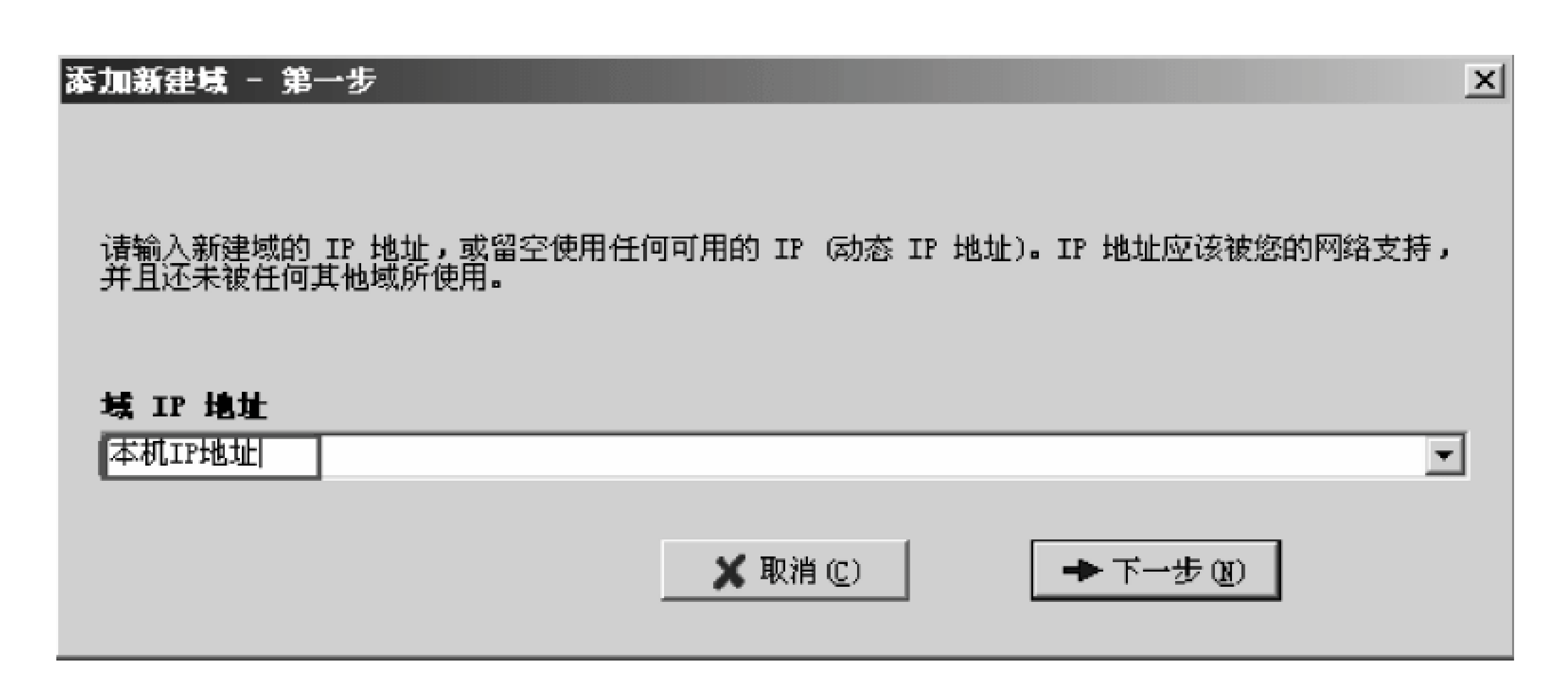


图 4.3 新建域

(3) 为新建域命名，输入域名，如图 4.4 所示，单击“下一步”按钮。

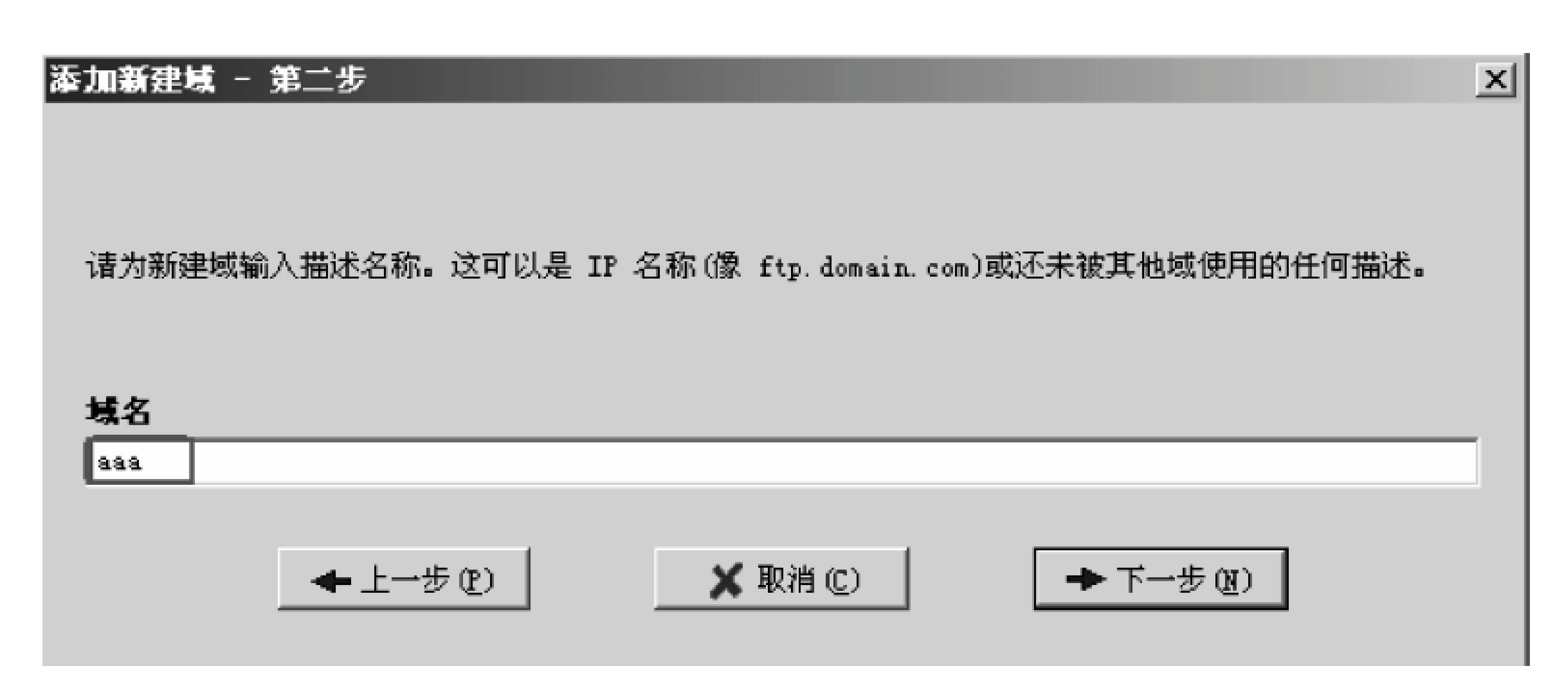


图 4.4 为新建域命名

(4) 设定 FTP 的端口，默认端口号为 21，如图 4.5 所示，单击“下一步”按钮。

(5) 设置“域类型”为存储于.ini 文件，如图 4.6 所示，然后单击“完成”按钮，域“aaa”就建好了。

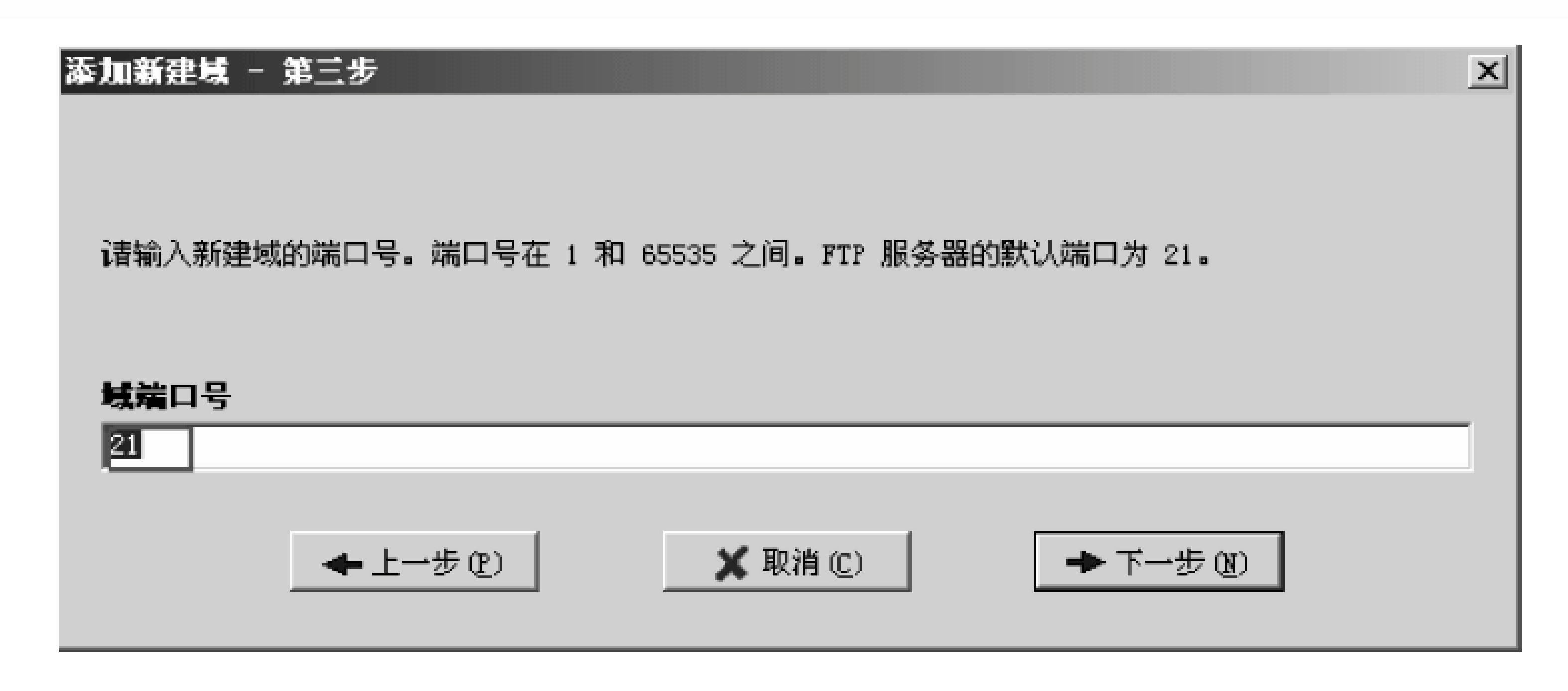


图 4.5　设定 FTP 端口

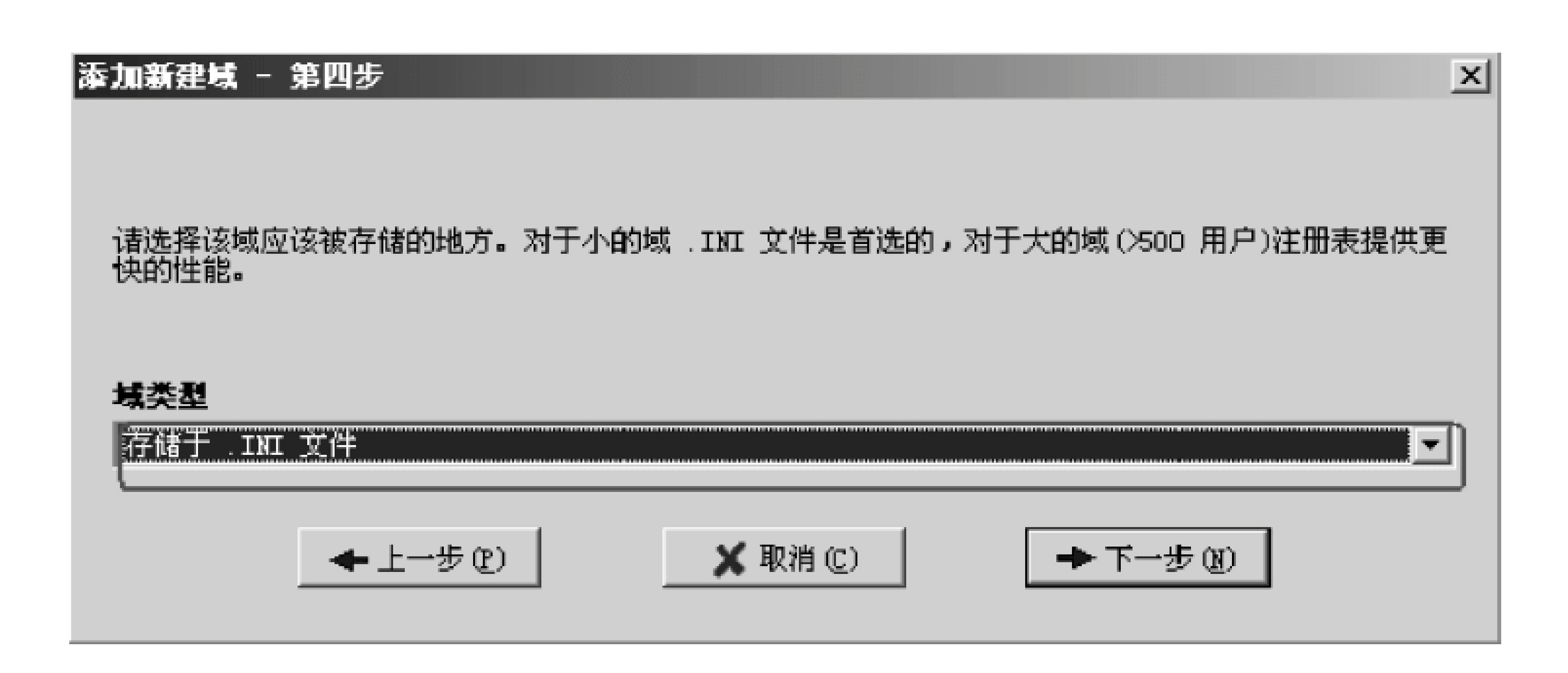


图 4.6　设置域类型

(6) 右击“用户”，在弹出的快捷菜单中选择“新建用户”选项，打开“添加新建用户”对话框，在“用户名称”输入 aaa，单击“下一步”按钮，如图 4.7 所示。

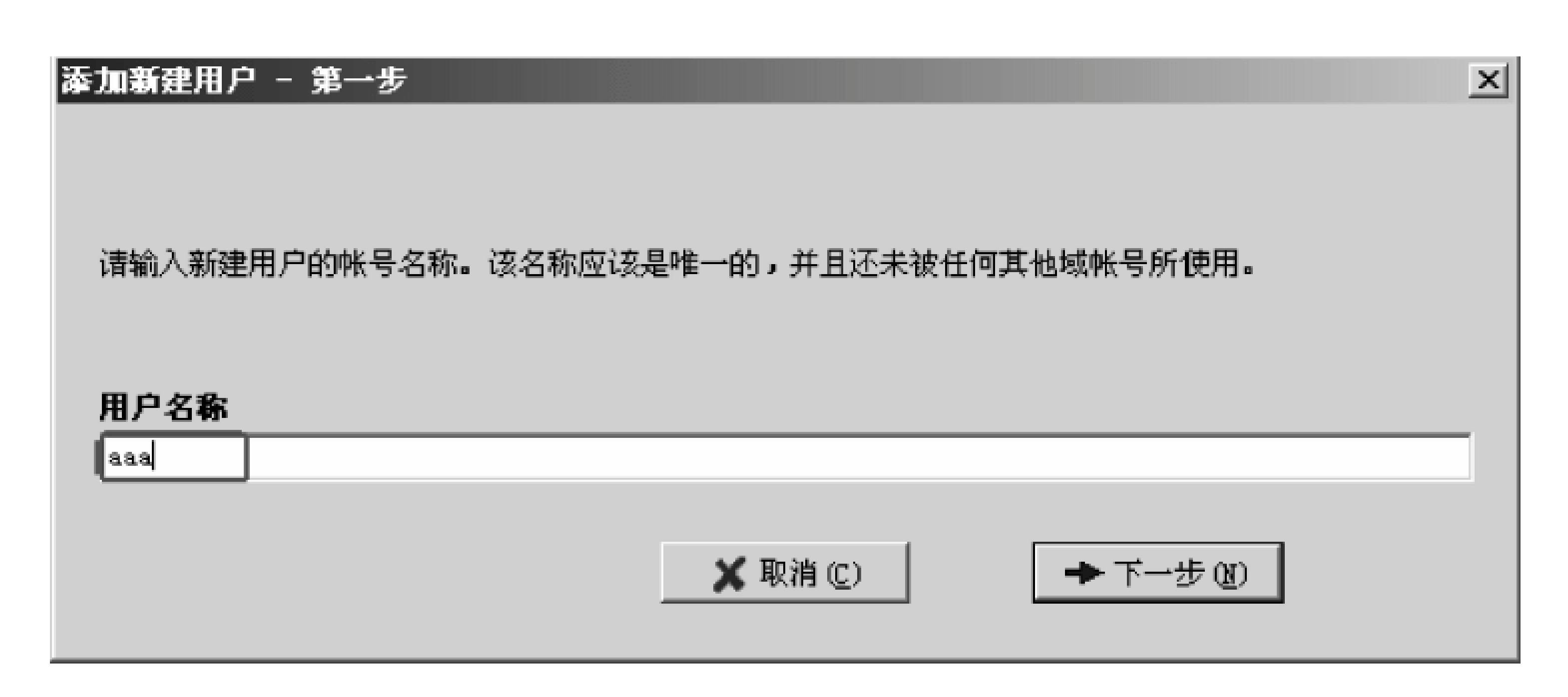


图 4.7　为新用户命名

(7) 为该用户设置密码“123”，单击“下一步”按钮，如图 4.8 所示。

(8) 为该用户设置主目录“C:\”，单击“下一步”按钮，如图 4.9 所示。

(9) 将用户锁定于主目录(用户登录 Serv-U FTP 后，只能操作该目录的文件)，如图 4.10 所示。



图 4.8　为新用户设定密码



图 4.9　为新用户设定主目录



图 4.10　锁定新用户的主目录

(10) 给用户分配文件、目录和子目录的读、写、执行等权限。单击"目录访问"按钮，在右侧复选框中设定读、写、列表、创建、移除等权限(注意：aaa 要赋予全部权限)，然后单击"应用"按钮，如图 4.11 所示。这样用户"aaa"就有了对目录、文件等相应的操作权限。

(11) 同样的办法，创建用户名"bbb"，密码"123"，但是给他分配权限只有读取、列表和继承的权限，即选中读取、列表、继承复选框。



图 4.11 给用户分配权限

(12) 在客户端 PC 上,打开浏览器,输入 FTP://192.168.1.251,登录 FTP 服务器,打开 FTP 登录界面,如图 4.12 所示。

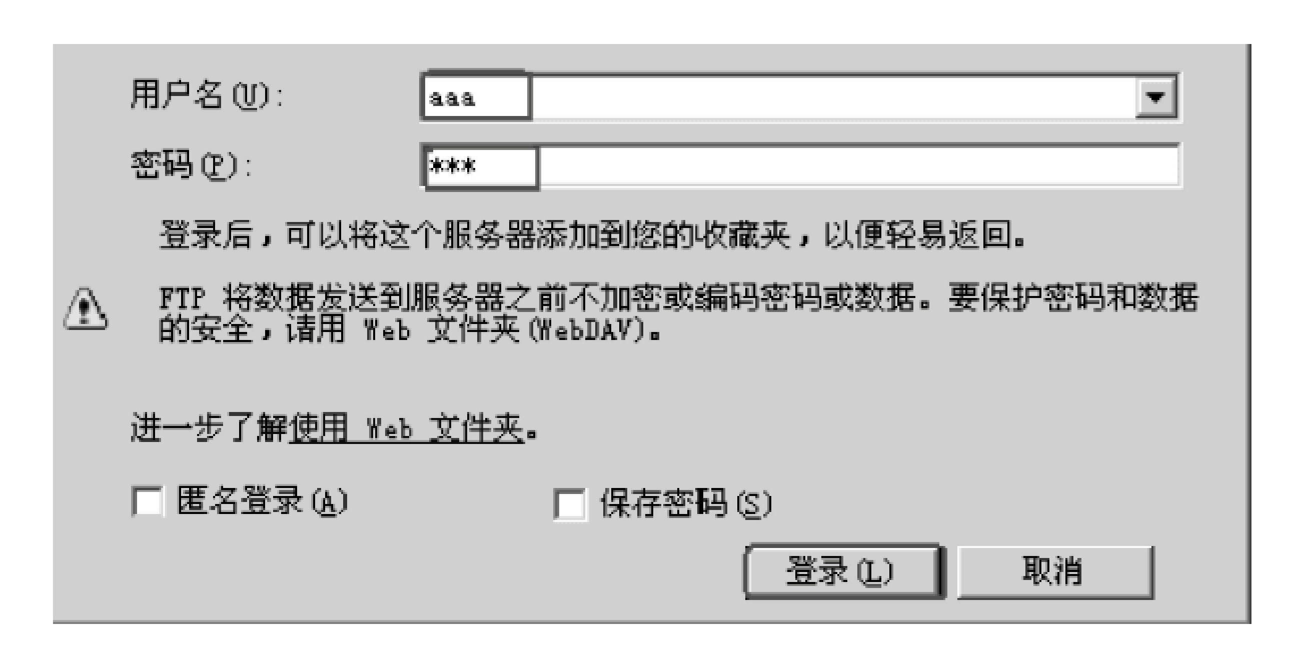


图 4.12 FTP 登录界面

以用户名“aaa”和密码“123”登录,登录成功后,创建一个“aaa”文件夹(能成功否?),如果能成功,在“aaa”文件夹再新建一个名为 aaa.txt 的文件(能成功否?),能否将“aaa”文件夹删除?为什么?

(13) 退出 aaa 登录,再以用户名“bbb”和密码“123”登录,登录成功后,创建一个“bbb”文件夹(能成功否?),为什么?

2) 用 SSL 加密增强 FTP 服务器安全性

PC 终端开启 Wireshark 软件,进行抓包(参考实验分析对比加密包)。

在以上 FTP 服务器的配置中,是以明文方式传输数据的,安全性极差,信息很容易被盗,为了保证特殊环境下的数据安全,有必要启用 SSL 功能。

不安全分析:设 FTP 服务器中有一个用户名“user”和密码“11111”。当用户在客户端 PC 上 URL 地址中输入 FTP://192.168.1.251,使用用户名“user”和密码“111111”,

访问 FTP 服务器 192.168.1.251 时，使用 Wireshark 软件进行抓包，抓包结果如图 4.13 所示。

```
⊞ Frame 1362 (103 bytes on wire, 103 bytes captured)
⊞ Ethernet II, Src: AsustekC_77:0a:dd (00:1f:c6:77:0a:dd), Dst: 50:78:8f:80:27:4b (50
⊞ Internet Protocol, Src: 192.168.100.5 (192.168.100.5), Dst: 192.168.100.2 (192.168.
⊟ Transmission Control Protocol, Src Port: ftp (21), Dst Port: onehome-help (2199), S
    Source port: ftp (21)
    Destination port: onehome-help (2199)
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 50    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x18 (PSH, ACK)
    Window size: 32768
  ⊞ Checksum: 0x49a4 [incorrect, should be 0x7ca0 (maybe caused by "TCP checksum offl
⊞ File Transfer Protocol (FTP)

0000  50 78 8f 80 27 4b 00 1f  c6 77 0a dd 08 00 45 00   Px..'K.. .w....E.
0010  00 59 12 9a 40 00 40 06  00 00 c0 a8 64 05 c0 a8   .Y..@.@. ....d...
0020  64 02 00 15 08 97 0a 35  23 77 9b 6d 9a 0b 50 18   d......5 #w.m..P.
0030  80 00 49 a4 00 00 32 32  30 20 53 65 72 76 2d 55   ..I...22 0 Serv-U
0040  20 46 54 50 20 53 65 72  76 65 72 20 76 36 2e 34    FTP Ser ver v6.4
0050  20 66 6f 72 20 57 69 6e  53 6f 63 6b 20 72 65 61    for Win Sock rea
0060  64 79 2e 2e 2e 0d 0a                               dy.....
```

图 4.13　使用 Wireshark 软件进行抓包

对抓包结果分析后(图 4.14)，用户在登录服务器的过程中，用户名和密码都被截获，这样，FTP 服务器就不安全了。

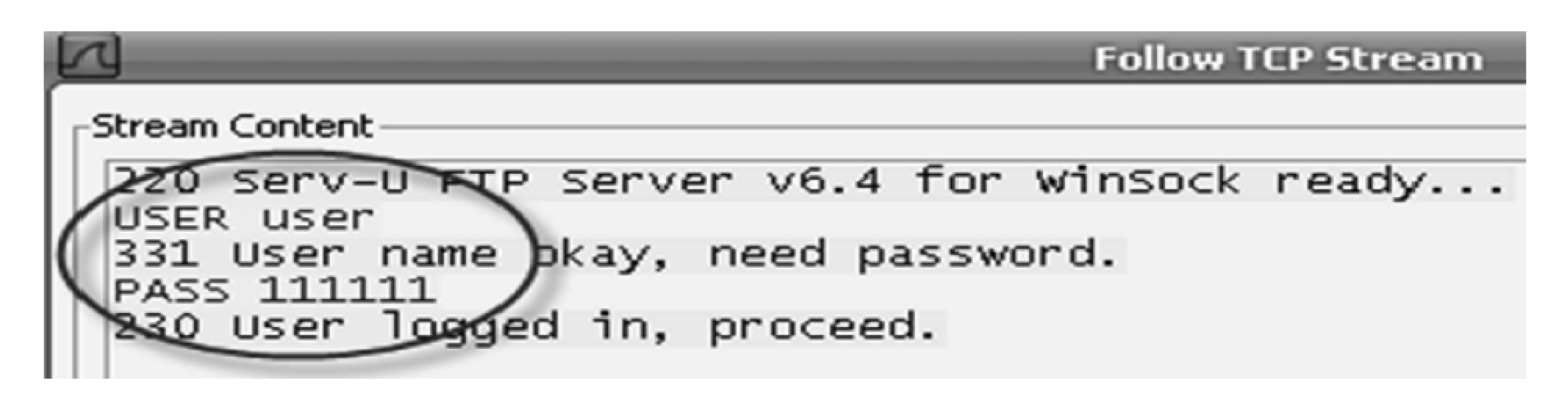


图 4.14　抓包分析结果

(1) 生成 SSL 证书。要想使用 Serv-U 的 SSL 功能，当然需要 SSL 证书的支持才行。虽然 Serv-U 在安装之时就已经自动生成了一个 SSL 证书，但这个默认生成的 SSL 证书在所有的 Serv-U 服务器中都是一样的，非常不安全，所以需要手工创建一个新的 SSL 证书。

在“Serv-U 管理员”窗口中，展开“本地服务器”→“设置”选项，然后切换到“SSL 证书”选项卡(图 4.15)，在这里创建一个新的 SSL 证书。首先在“普通名称”栏中输入一个名称(可以输入 FTP 服务器的 IP 地址)，接着其他栏目的内容，如电子邮件、组织和单位等，根据用户的情况进行填写，完成“SSL 证书”选项卡中所有内容的填写后，单击下方的“应用”按钮即可，这时 Serv-U 就会生成一个新的 SSL 证书。



图 4.15　创建一个新的 SSL 证书

（2）启用 SSL 功能。虽然为 Serv-U 服务器创建了新的 SSL 证书，但默认情况下，Serv-U 是没有启用 SSL 功能的，要想利用该 SSL 证书，首先要启用 Serv-U 的 SSL 功能才行。

如启用 Serv-U 服务器中域名为“welcome”的 SSL 功能。在“Serv-U 管理员”窗口中，依次展开“本地服务器”→“域”→“welcome”选项，然后在右侧的“域”管理框中找到“安全性”下拉列表框中的选项。这里 Serv-U 提供了 3 种选项，分别是“仅仅规则 FTP，无 SSL/TLS 进程”、“允许 SSL/TLS 和规则进程”、“只允许 SSL/TLS 会话”，默认情况下，Serv-U 使用的是“仅仅规则 FTP，无 SSL/TLS 进程”，因此是没有启用 SSL 加密功能的。在这里“安全性”下拉选项框中选择“只允许 SSL/TLS 会话”选项，然后单击“应用”按钮，即可启用 welcom 域的 SSL 功能，如图 4.16 所示。

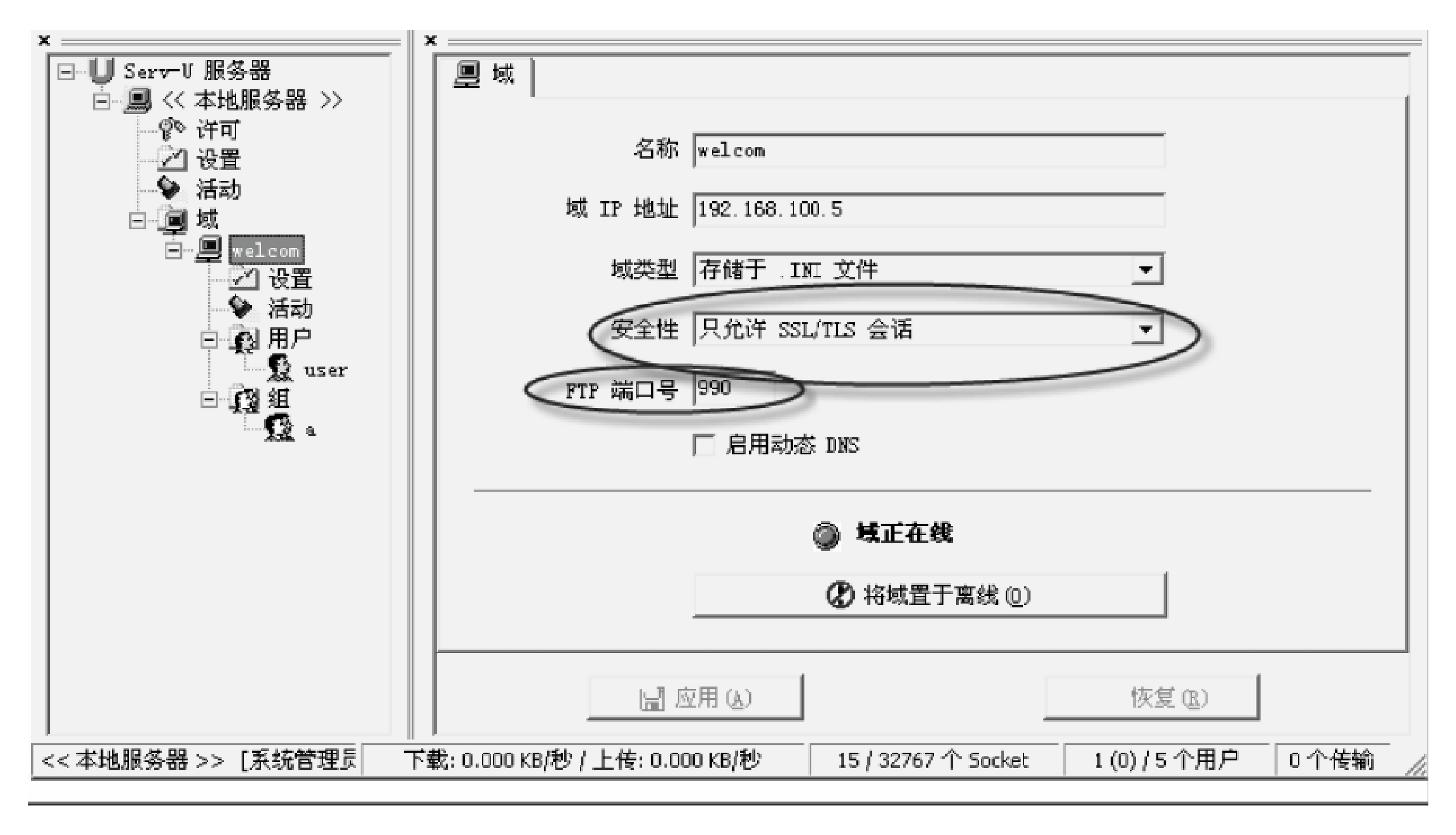


图 4.16　启用 SSL 功能

注意：启用了 SSL 功能后，Serv-U 服务器使用的默认端口号就不再是“21”了，而是“990”了。这点 FTP 用户一定要留意，否则就会无法成功连接 Serv-U 服务器。

(3) SSL 应用。启用 Serv-U 服务器的 SSL 功能后，就可以利用此功能安全传输数据了，但 FTP 客户端程序必须支持 SSL 功能才行。

支持 SSL 的 FTP 客户端程序现在也比较多，以“FlashFXP”程序为例，介绍如何成功连接到启用了 SSL 功能的 Serv-U 服务器。在客户端运行“FlashFXP”程序后，选择“会话”→“快速连接”选项，弹出“快速连接”对话框，在“服务器或 URL”栏中输入 Serv-U 服务器的 IP 地址(之前做了配置)，在“端口”栏中一定要输入“990”，这是因为 Serv-U 服务器启用 SSL 功能后，端口号就从“21”变为“990”；接着在“用户名”和“密码”栏中输入用户的登录账号和密码。

(4) 切换到“SSL”选项卡，选中“绝对 SSL”单选按钮，这一步骤是非常关键的，如果不选中“绝对 SSL”单选按钮，就无法成功连接到 Serv-U 服务器。最后单击“连接”按钮，如图 4.17 所示。



图 4.17 启用绝对 SSL 功能

(5) 当用户第一次连接到 Serv-U 服务器时，FlashFXP 会弹出一个“证书”对话框，这时用户只要单击“接受并保存”按钮，将 SSL 证书下载到本地后，就能成功连接到 Serv-U 服务器，以后和 Serv-U 服务器间的数据传送就会受到 SSL 功能的保护，不再是以明文形式传送，这样就不用再担心 FTP 账号被盗，敏感信息被窃取的问题了。

在启用了 SSL 后，使用 Wireshark 仍可截获的 FTP 包，但此时用户登录的信息等已经被加密了。截获的包是一堆乱码，如图 4.18 所示。

3. 思考题

(1) 考虑 FTP 的默认端口：21、20 各有什么作用，请测试检验，形成实验报告。

(2) 如何在 IIS 中配置安全的 FTP 服务，形成实验报告。

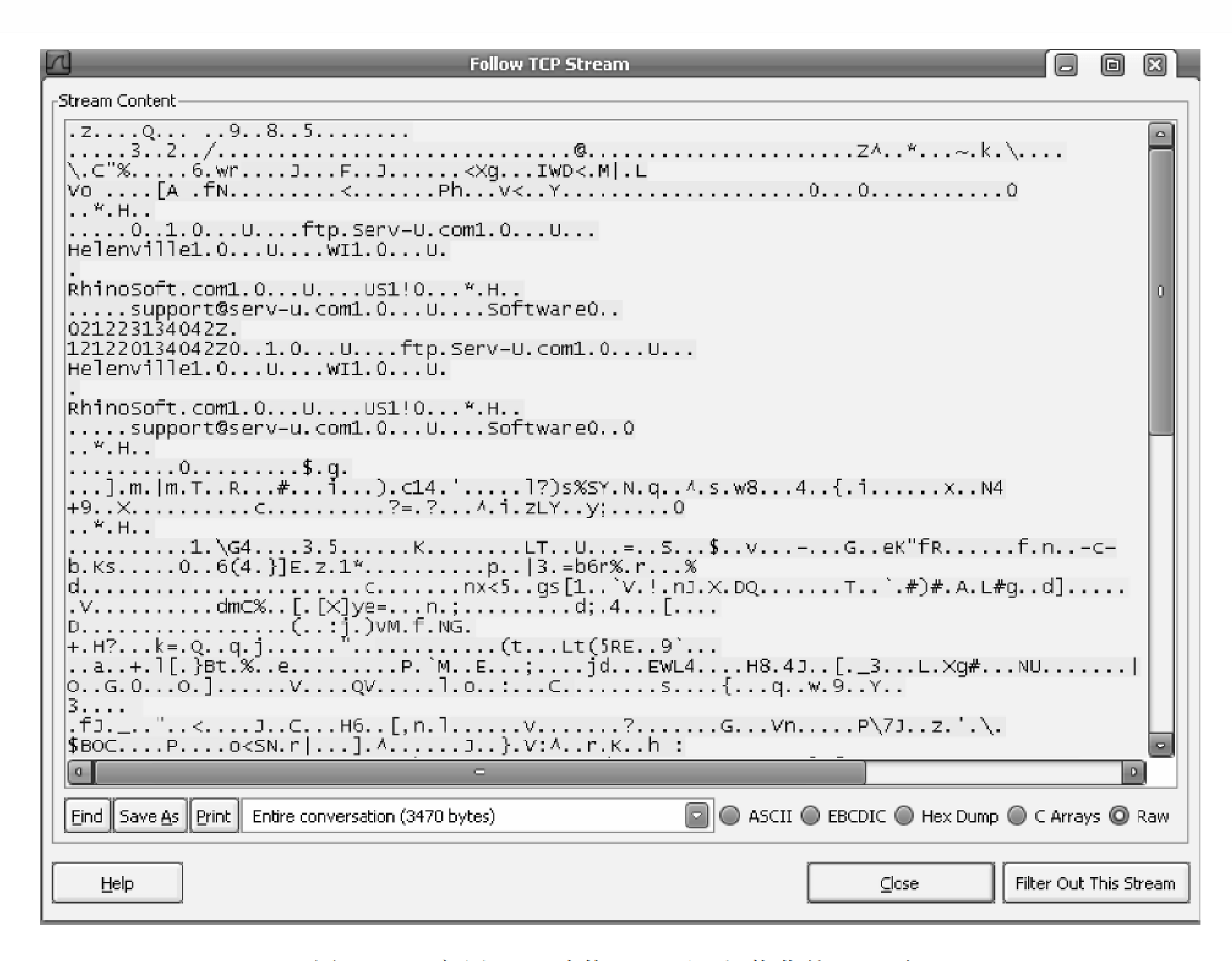
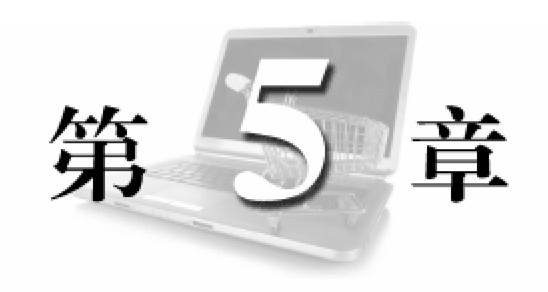


图 4.18　启用 SSL 功能 Wireshark 截获的 FTP 包



第5章 数据库篇

5.1 引言

随着全球信息化进程加速，计算机网络的规模飞速扩大，作为信息载体的数据库已经深入到社会的政治、经济、文化、军事和社会生活等各个方面，其安全已成为世界各国共同关注的焦点。传统的数据库安全技术已经不能满足现实的要求，数据库账户管理和安全审计技术开始广泛受到人们的重视。

数据库(Database)是一个单位或是一个应用领域的通用数据存储处理系统，它存储的是属于企业、事业、部门、团体和个人的有关数据的集合。它产生于距今50年前，随着信息技术和市场的发展，特别是20世纪90年代以后，数据管理不再仅仅是存储和管理数据，而转变成用户所需要的各种数据管理的方式。数据库有很多种类型，从最简单的存储有各种数据的表格到能够进行海量数据存储的大型数据库系统。数据库在各个方面都得到了广泛的应用。

数据库中的数据是为众多用户共享其信息而建立的，已经摆脱了具体程序的限制和制约。不同的用户可以按各自的用法使用数据库中的数据；多个用户可以同时共享数据库中的数据资源，即不同的用户可以同时存取数据库中的同一个数据。数据共享性不仅满足了各用户对信息内容的要求，同时也满足了各用户之间信息通信的要求。

5.2 SQL Server 概述

数据库必须具有坚固的安全系统，才能控制可以执行的活动以及可以查看和修改的信息。无论用户如何获得对数据库的访问权限，坚固的安全系统都可以确保对数据进行保护。安全系统的构架建立在用户组的基础上。

5.2.1 SQL Server 的安全设置

在 SQL Server 中，用户要经过两个安全性阶段：身份验证和授权。身份验证能决定用户能否连接到服务器，授权阶段验证已登录服务器的用户能否连接 SQL Server 实例的权限。

5.2.2 SQL Server 的身份验证模式

SQL Server 服务器身份验证有两种模式：Windows 认证模式和 Windows 与 SQL Server 混合认证模式。Windows 认证更为安全，因为 Windows 操作系统具有较高的安全性(C2 级安全标准)。SQL Server 认证管理较为简单，当 SQL Server 在 Windows NT 或 Windows 2000 上运行时，系统管理员必须制定系统使用的认证模式。当采用混合认证模式时，SQL Server 既允许使用 Windows 认证模式又允许使用 SQL Server 认证模式。在完成 SQL Server 安装以后，SQL Server 就建立了一个特殊账户 sa。账户 sa 拥有最高的管理权限，可以执行服务器范围内的所有操作，既不能更改 sa 用户名称，也不能删除 sa，但可以更改其密码。在刚刚完成 SQL Server 的安装时，sa 账户没有任何密码，所以要尽快为其设置密码。

5.2.3 授权阶段

只有授权的用户才能访问被保护了的数据，保密性是防止非授权访问，这是信息安全最重要的要求。用户在实现安全登录之后，检验用户的下一个安全等级是数据库访问权限。在身份验证阶段利用登录账号连接到服务器后，只表明该账户通过了 Windows NT 认证或 SQL Server 认证，并不代表用户就能访问数据库，而登录者要操作数据库中的数据时，必须要有用户账号才能够存取数据库。就如同在自助银行门口刷卡进门(登录服务器)，然后再凭银行卡和密码支取现金(进入数据库)一样。数据库用户是指在数据库内唯一标识用户身份的 ID。SQL Server 通过授权和角色管理来给用户指定可以访问的数据库对象的权限。如果一组用户具有相同的权限，那么可以先创建一个角色，对这个角色赋予权限，然后将这些用户添加到该角色中使它们成为这个角色的成员。这样就可以对这些相同权限的用户进行统一的管理，在用户较多的情况下可减轻管理负担。在 SQL Server 中，系统的每个数据库都定义了许多不同的固定角色，但这些角色的范围只限于它所在的数据库。每个用户可以属于多个不同的角色，从而拥有不同的权限。

5.3 数据库审计

作为信息安全审计的重要组成部分，同时也是数据库管理系统安全性重要的部分。通过审计功能，凡是与数据库安全性相关的操作均可被记录下来。只要检测审计记录，系统安全员便可掌握数据库被使用状况。例如，检查库中实体的存取模式，监测指定用户的行为。审计系统可以跟踪用户的全部操作，这也使审计系统具有一种威慑力，提醒

用户安全使用数据库。现有的数据库管理系统的审计保护功能存在不足，应从以下两方面改进：一是建立单独的审计系统和审计员，审计数据需要存放在单独的审计文件中。可以把用户大致分为审计员、数据库用户、系统安全员3类，这三者相互牵制、各司其职，分别在3个地方进行审计控制。二是为了保证数据库系统的安全审计功能，还需要考虑到系统能够对安全侵害事件做出自动响应，提供审计自动报警功能。当系统检测到有危害到系统安全的事件发生并达到预定的阈值时，要给出报警信息，同时还应自动断开用户的连接，终止服务器端的相应线程，并阻止该用户再次登录系统。

5.4 触发器

触发器是一种特殊的存储过程，类似于其他编程语言中的事件函数，SQL Server 允许为 INSERT、UPDATE、DELETE 创建触发器，当在表(视图)中插入、更新、删除记录时，触发一个或一系列 T-SQL 语句。SQL Server 的触发器按触发方式可分为 DML 触发器和 DDL 触发器两大类。DML 触发器的特点是当数据库中发生 DML(数据操作语言)事件时被触发。数据操作语言事件包括在指定表或视图中插入、更新、删除记录。DML 触发器被广泛应用于数据被修改时强制执行业务规则，以及数据完整性检查。DDL 触发器是 SQL Server 2005 的新增功能，当服务器或数据库中发生 DDL(数据定义语言)事件时将调用该触发器。SQL Server 的触发器按触发时机可分为 AFTER 触发器和 INSTEADOF 触发器两种类型。AFTER 触发器是指相应的操作被执行完毕后触发。INSTEADOF 触发器是指在相应的操作被执行前触发并替代该操作。SQL Server 的触发器按触发类型可分为 INSERT 触发器、DELETE 触发器和 UPDATE 触发器三类。当 INSERT 触发器被触发时，系统会建立一个名为 inserted 的逻辑表，被插入的数据行会被复制到 inserted 中。当 DELETE 触发器被触发时，系统会建立一个名为 deleted 的逻辑表，被删除的数据行会被复制到 deleted 中。当 UPDATE 触发器被触发时，系统会分别建立名为 deleted、inserted 的逻辑表，更新前的数据行会被复制到 deleted 中，更新后的数据行将被复制到 inserted 中。因此，UPDATE 触发器可以理解为先 DELETE 了旧的数据行，再 INSERT 新的数据行。

在编写触发器过程中，可以使用 UPDATE(column)来判断在指定的列上是否进行了 INSERT 或 UPDATE 操作。也可以使用 COLUMNS_UPDATED()来判断是否插入或更新了提及的列。这两种方法都是仅能用于 INSERT 或 UPDATE 触发器中，不能在 DELETE 触发器中使用。

实验 8 数据库账户管理实验

一、实验目的

通过本实验，充分了解账户控制对于整个应用安全的重要性。尤其是在分配账户时需要注意的各个方面，以确保将来使用系统过程中的基础安全特性。

二、实验原理

SQL Server 的服务器级安全性建立在控制服务器登录账户和密码的基础上。SQL Server 采用了标准的 SQL Server 登录和 Windows 登录两种方式。无论使用哪种方式登录，用户在登录时提供的登录账户和密码都决定了该用户能否获得 SQL Server 的访问权，以及在获得访问权以后用户的访问资源及可用的权利和内容对象。管理和设计合理的登录账户是 SQL Server 系统管理员的重要任务。

三、实验内容

1. 实验环境

(1) 硬件设备：小组 PC(Windows Server 2003 系统)一台。

(2) 软件工具：SQL Server 2005。

2. 实验步骤

1) 设定 sa 的密码

(1) 获取本机的主机名：执行"开始"→"运行"命令，在打开的"运行"对话框中输入"cmd"，在命令行窗口中输入"hostname"命令，记录系统显示(后面登录时要用主机名)。

(2) 启动 SQL Server Management Studio：执行"开始"→"所有程序"→Microsoft SQL Server 2005→SQL Server Management Studio 命令。

(3) 连接服务器：当出现"连接到服务器"窗口后，服务器类型选择"数据库引擎"，服务器名称选择自己的主机名(在步骤(1)中获得)。身份验证选择"Windows 身份验证"，然后单击"连接"按钮，成功后，将打开数据库服务器管理窗口，如图 5.1 所示。

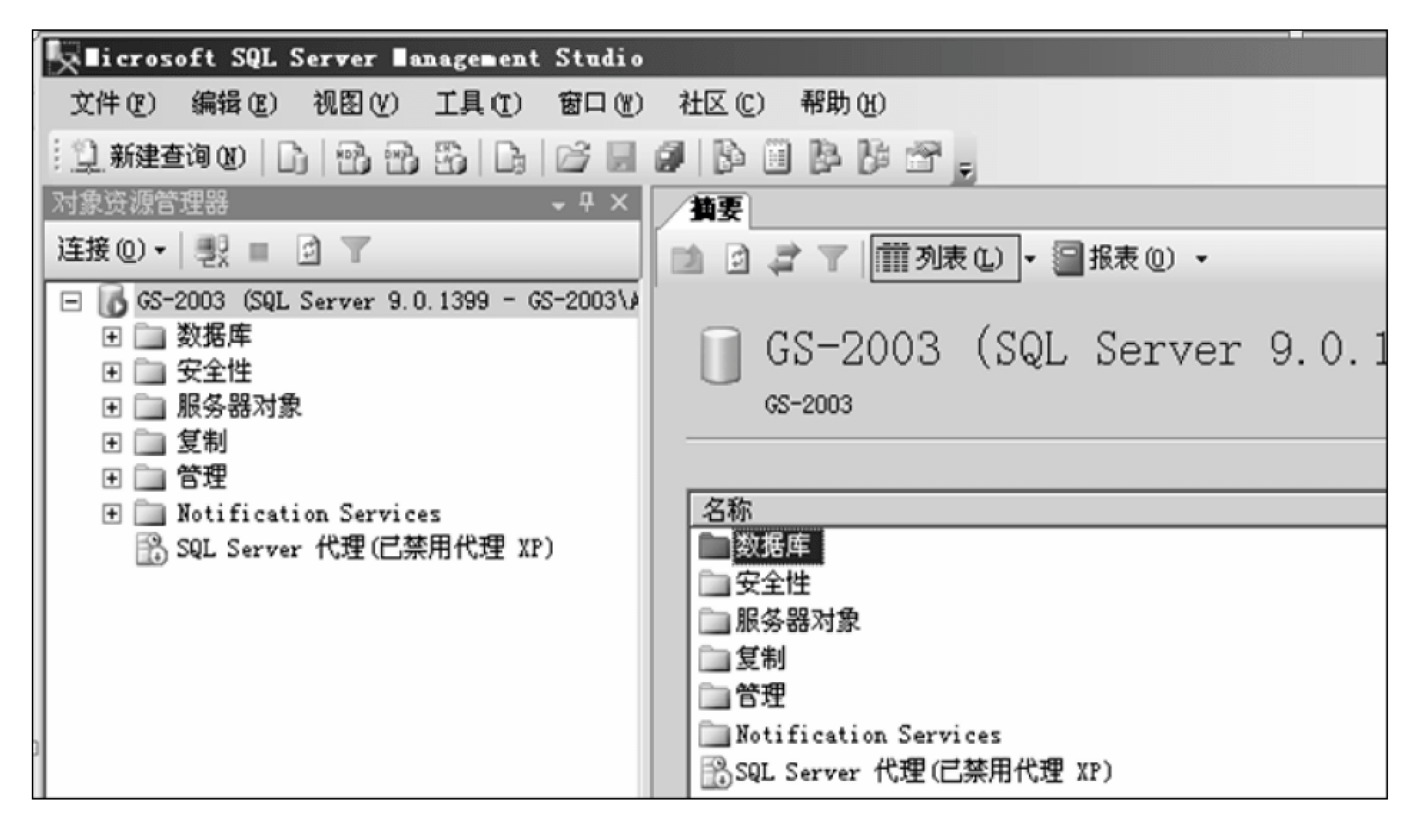


图 5.1 数据库服务器管理窗口

(4) 设定 sa 的密码：在“对象资源管理器”窗体中，展开“安全性”→“登录名”→“sa”选项，然后右击，在弹出的快捷菜单中选择“登录属性”选项，在“登录属性”窗口中的“常规”选项卡中，为 sa 修改登录密码(密码为 shanghai_sbs)，如图 5.2 所示。



图 5.2 修改 sa 登录密码

2) 登录账户管理配置

使用 SQL Server 身份证连接服务器时，用户必须有有效的 SQL Server 2005 登录账户和密码。建立用户登录账户的方式有两种：通过 SQL Server Management Studio 的图形界面进行创建；通过 SQL 语句建立。

(1) 打开“SQL Server Management Studio”，用 sa 进行登录，sa 的密码已在前面的步骤(4)中设定。

(2) 进入数据库服务器管理窗口后展开“安全性”→“登录名”选项，然后右击，在弹出的快捷菜单中选择“新建”选项，打开“登录名-新建”窗口，在“常规”中设置账户信息，这些信息将包含登录名、身份验证、默认数据库及语言。由于它们都将涉及重要数据库安全要素，因此必须在这里对密码等信息严格设置，尽量采用复杂密码，即大于或等于 13 位，带有数字、字母、符号的信息，如 123abc＃＄rhhg988。同时也尽量使用 SQL Server 身份验证，避免与 Windows 混用，杜绝非授权的系统用户篡改数据库的可能性。在新建登录窗口中输入用户名“user1”，为了测试简单，设置简单密码“user1”，默认数据库选择“master”，默认语言选择“simplifiedChinese”，单击“确定”按钮，新建 user1 成功，将看到左边的登录名下多了一个 user1 账户。

(3) 在图 5.3 所示的 SQL Server Management Studio 的图形界面中，单击工具栏的“新建查询”按钮，在弹出的 SQL 命令编辑窗口中输入：

```
execsp_addlogin 'user2','user2','master','simplifiedchinese'
```

(4) 检查语法单击 ✓ 按钮，运行单击 ! 执行(X) 按钮。返回值是“命令已成功完成”，即成功创建。重新启动 SQL Server Management Studio，检查用户情况。

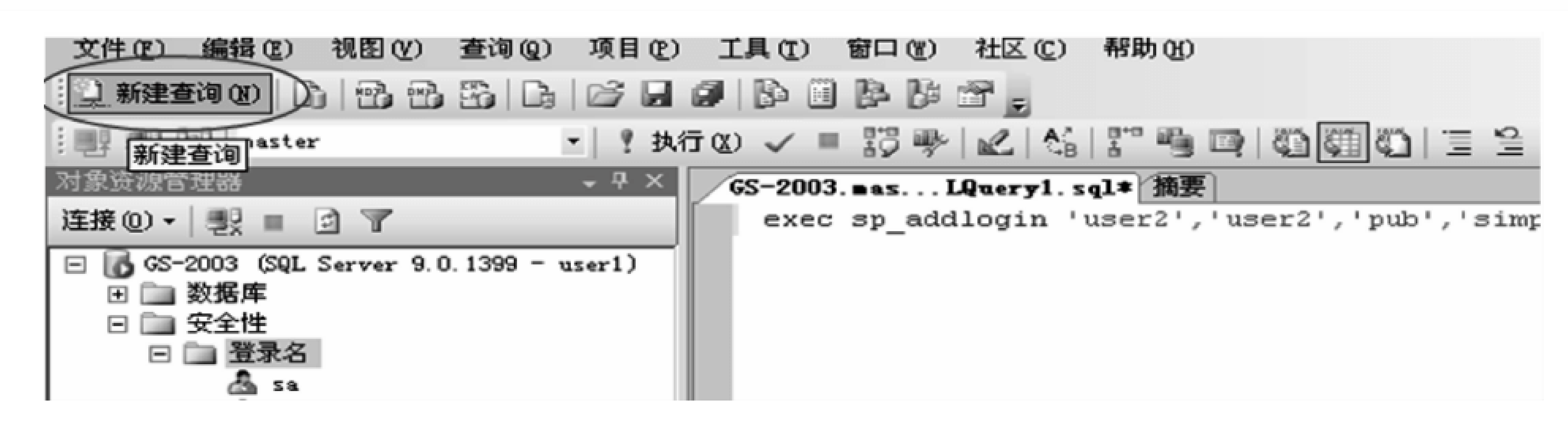


图 5.3　新建用户

(5) 设置服务器角色。用 sa 登录名登录，新建 user3 登录名，为测试简单，密码也是 user3，设置 user3 的服务器角色为所有，如图 5.4 所示。



图 5.4　设定用户角色

(6) 重新启动 SQL Server Management Studio，用 user3 登录，其窗口如图 5.5 所示。



图 5.5　用 user3 登录

(7) 用前面的 SQL 命令创建的 user2 用户进行登录，出现如图 5.6 所示的窗口，可见，在不同的服务器角色中，命令的限定将影响实际使用中的操作效果，这点必须在将来的实际环境中引起重视。



图 5.6 用 user2 登录

3. 思考题

查资料对比以下各种服务器角色代表的含义。

- bulkadmin
- dbcreator
- diskadmin
- processadmin
- securityadmin
- serveradmin
- setupadmin
- sysadmin

实验 9 数据库审计实验

一、实验目的

学会利用触发器，制作基于函数的数据库操作审计工具。更加深入理解 T-SQL 在数据库中的运用和意义，对数据库安全产生更加立体的认知。

二、实验原理

在工作中，对数据改变情况进行审计是很重要的，尤其是正在处理的机密信息。除了跟踪被改变的数据外，跟踪单个字段名称的改变也十分有用。这些信息对审计部门尤其重要，而且当调试数据库代码时也十分有用。

在建立审计表之前，有必要对触发器这一数据库对象进行必要的了解。

触发器(Trigger)是个特殊的存储过程，它的执行不是由程序调用，也不是手工启动，而是由事件来触发，例如，当对一个表进行操作(INSERT、DELETE、UPDATE)时就会

激活它执行。触发器经常用于加强数据的完整性约束和业务规则等。触发器可以从DBA_TRIGGERS,USER_TRIGGERS数据字典中查到。

利用触发器的功能,我们就可以对某个表建立审计表了,当对一个表进行INSERT、DELETE、UPDATE等操作时,利用触发器就可以将对数据表的更改信息存入审计表,从而达到对关键数据库进行更改跟踪的目的。

三、实验内容

1. 实验环境

(1) 硬件设备:小组PC(Windows Server 2003系统)一台。

(2) 软件工具:SQL Server 2005。

2. 实验步骤

(1) 打开Microsoft SQL Server Management Studio,用sa账户进行登录,出现如图5.7所示的窗口。



图5.7　用sa登录

(2) 右击数据库图标,选择新建数据库,数据库名称为TestAudit,所有者为sa,如图5.8所示。

脚本 · 帮助

数据库名称(N): TestAudit

所有者(O): sa

使用全文索引(U)

数据库文件(F):

逻辑名称	文件类型	文件组	初始大小(MB)	自动增长	路径
TestAudit	数据	PRIMARY	3	增量为 1 MB,不限制增长	C:\Program Files\Micr
TestAudit...	日志	不适用	1	增量为 10%,不限制增长	C:\Program Files\Micr

图5.8　新建TestAudit数据库

(3) 单击工具栏的“新建查询”按钮，在出现的 SQL 语句编辑窗口中输入如下语句，单击 ✓ 按钮分析代码是否有语法错误，单击 ! 执行(X) 按钮将建立数据库表和审计表。

```
useTestAudit
go

/＊建立数据库表 grades＊/
createtablegrades(
studentIDint,
courseIDint,
gradeint,
primarykey(studentID,courseID)
);
/＊建立审计表 audit,对数据库表 grades 的更改情况进行记录＊/
createtableaudit(
changeTypechar(15),
changeTimedatetime,
studentIDint,
courseIDint,
gradeint,
primarykey(changeType,changeTime,studentID,courseID,grade)
)
```

(4) 建立触发器(图 5.9)，将对 grades 表的修改记录存入审计表 audit 中。

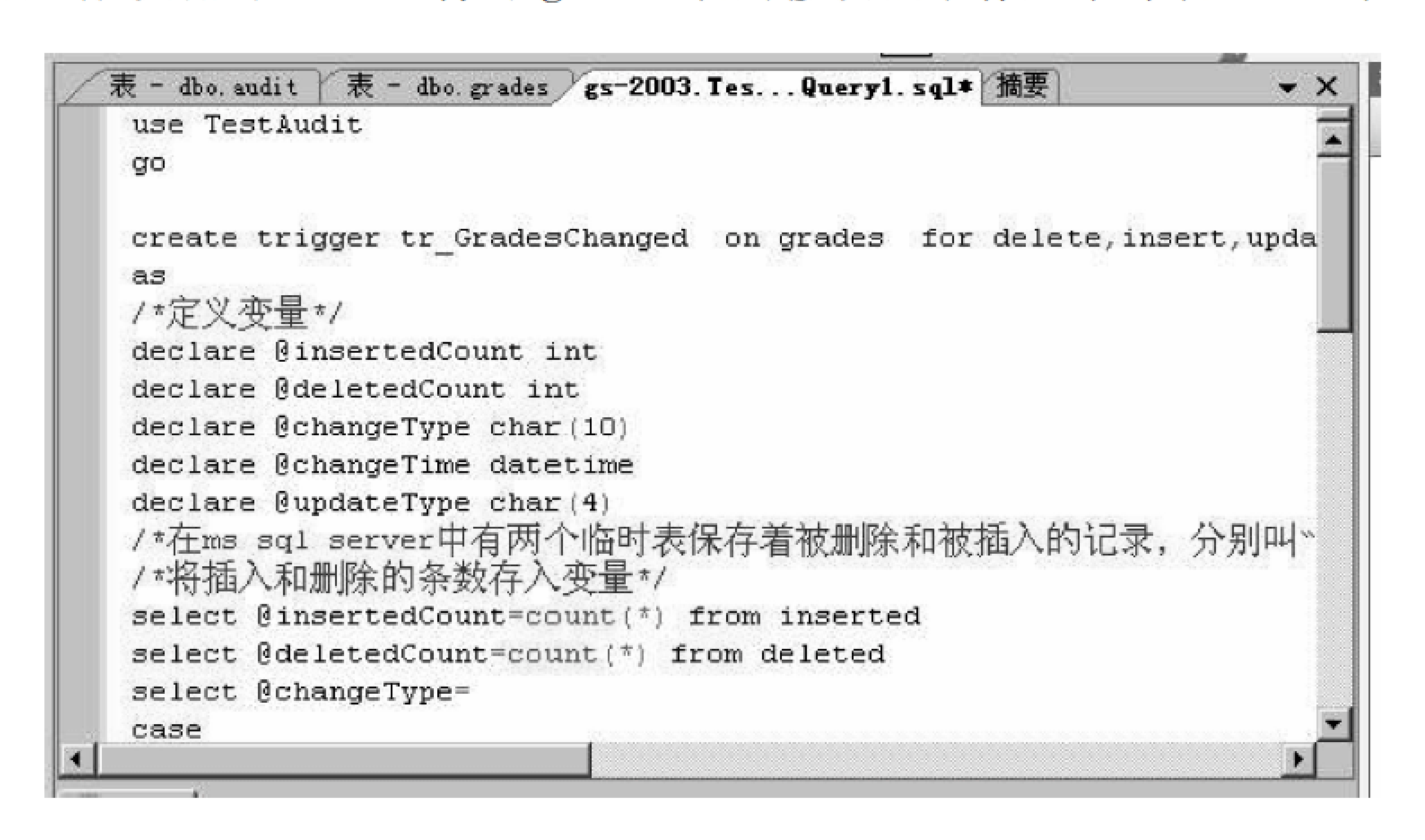


图 5.9 触发器

代码如下：

```
/＊创建触发器＊/
createtriggertr_GradesChangedongradesfordelete,insert,update
as
/＊定义变量＊/
```

```
declare@insertedCountint
declare@deletedCountint
declare@changeTypechar(10)
declare@changeTimedatetime
declare@updateTypechar(4)
/*在 mssqlserver 中有两个临时表保存着被删除和被插入的记录,分别叫"deleted",
"inserted".update 可以看做一次删除和一次添加*/
/*将插入和删除的条数存入变量*/
select@insertedCount=count(*)frominserted
select@deletedCount=count(*)fromdeleted
select@changeType=
case
when@insertedCount>0and@deletedCount>0
then'update'
when@insertedCount=0and@deletedCount>0
then'delete'
else'insert'
end
select@changeTime=getdate()
select@updateType=''
if@changeType='update'select@updateType='old'
/*将对数据库表 grades 的更改记录存入审计表中*/
insertintoaudit(changeType, changeTime, studentID, courseID, grade) select @ changeType +
@updateType,@changeTime,studentID,courseID,gradefromdeleted
if@changeType='insert'select@updateType='new'
insertintoaudit(changeType, changeTime, studentID, courseID, grade) select @ changeType +
@updateType,@changeTime,studentID,courseID,gradefrominserted
```

(5) 对数据库表 grades 进行 INSERT、UPDATE 和 DELETE 操作,查看审计表 audit 的变化情况,如图 5.10 所示。

表 - dbo.audit | 表 - dbo.grades | gs-2003.Tes...Qu

	studentID	courseID	grade
	11	21	87
	12	22	98
	13	23	57
*	NULL	NULL	NULL

(a)

表 - dbo.audit | 表 - dbo.grades | gs-2003.Tes...Query1.sql* | 摘要

	changeType	changeTime	studentID	courseID	grade
▶	insert new	2010-7-20 17:1...	1	1	87
	insert new	2010-7-20 17:1...	12	22	98
	update old	2010-7-20 17:1...	1	1	87
	update old	2010-7-20 17:1...	11	21	87
*	NULL	NULL	NULL	NULL	NULL

(b)

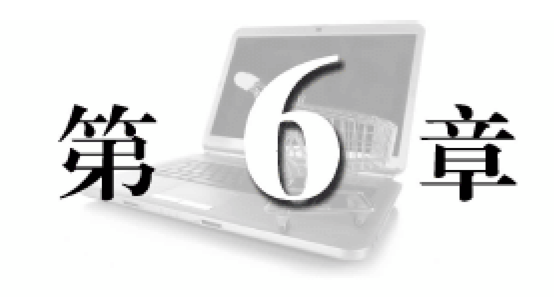
图 5.10 审计表

从表5.10中,可以看到,通过对数据表的INSERT和UPDATE操作后,在审计表audit中产生了相关记录。

3. 思考题

(1) 根据上文的审计表的建立方法,设计一个能够记录登录账户名称的审计表。

(2) 上网查找资料,一个完整的审计表需要包含哪些要素,并通过实验建立包含完整要素的审计表。

第  章

电子商务应用篇

6.1 引言

电子商务是指采用数字化电子方式进行商务数据交换和开展的商务业务活动。它是在全球各地广泛的商业贸易活动中，在因特网开放的网络环境下，基于浏览器/服务器应用方式，买卖双方不谋面地进行各种商贸活动，实现消费者的网上购物、商户之间的网上交易和在线电子支付，以及各种商务活动、交易活动、金融活动和相关的综合服务活动的一种新型的商业运营模式。电子商务系统是涉及商务活动的各方，包括商店、消费者、银行或金融机构、信息公司或证券公司和政府等，利用计算机网络技术全面实现在线交易电子化的过程。电子商务系统的关键在于完全实现在线支付功能，所以为了顺利完成整个交易过程，不仅需要建立电子商务服务系统、通用的电子交易支付方法和机制，还要确实保证参加交易各方和所有合作伙伴都能够安全可靠地进行全部商业活动。

由于电子商务是在 Internet 等网络上进行的，因此，网络是电子商务最基本的构架。电子商务还强调使系统的软件和硬件、参加交易的买方、卖方、银行或金融机构、厂商、企业和所有合作伙伴，都要在 Internet、Intranet、Extranet 中密切结合起来，共同从事在网络计算环境下的商业电子化应用。

电子商务经过十来年的快速发展，现在可以毫不夸张地说，它已经成为国家社会经济建设的一个基本组成部分和国家未来的重点发展方向。越来越多的企业活动和个人行为都不得不依靠电子商务来完成，人们对电子商务的认识和接受也从初期的阳春白雪进入到现在大众化的阶段。

借助网络进行电子交易是电子商务实施的重要环节。对于网上交易而言，通信、计算机、电子支付以及安全等现代信息技术是其实现的保证。网上交易的过程如图 6.1 所示。

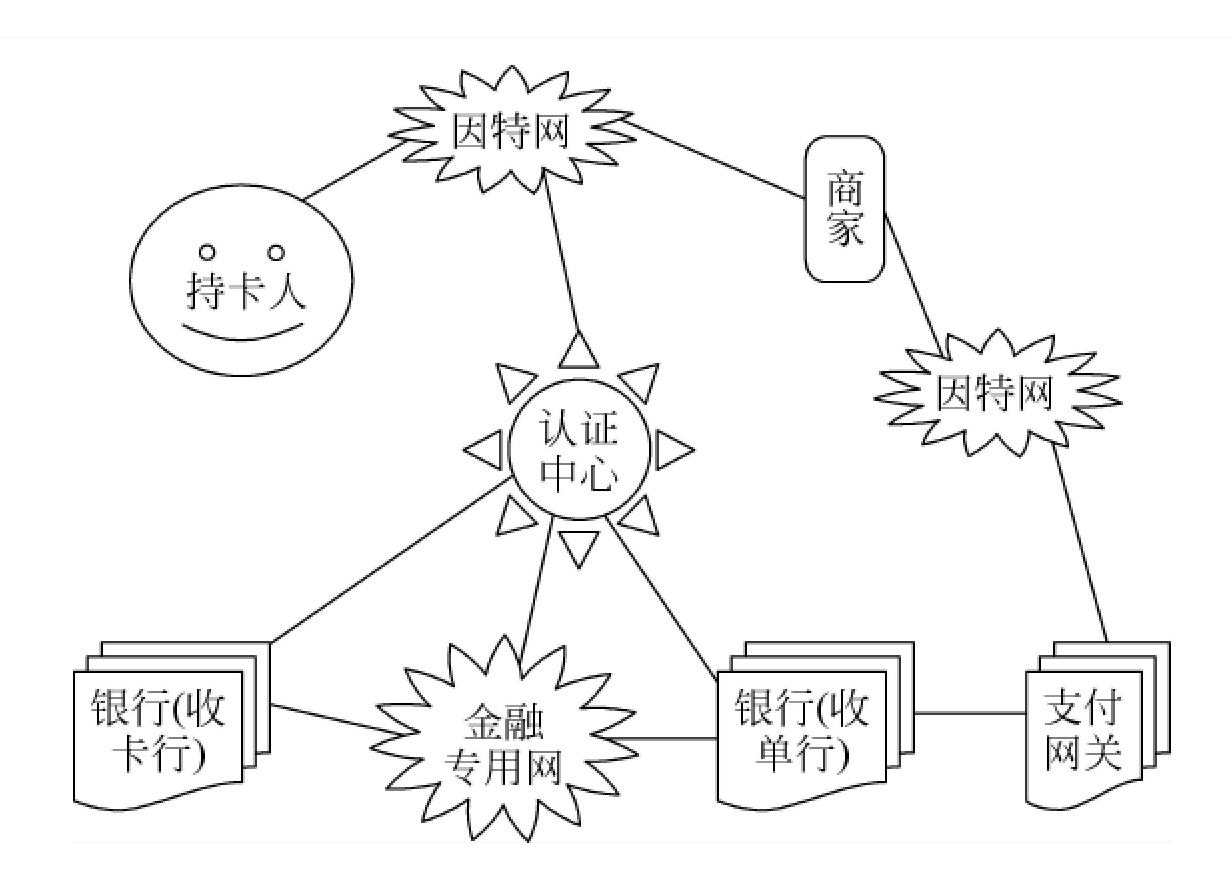


图 6.1 电子商务网上交易示意图

消费者向商家发出购物请求，商家把消费者的支付指令通过支付网关（负责将持卡人的账户中的资金转入商家账户的金融机构，由金融机构或第三方控制，处理持卡人购买和商家支付的请求）送往商家的收单行，收单行通过银行卡网络从发卡行（消费者开户行）取得授权后，把授权信息通过支付网关送回商家，商家取得授权后，向消费者发送购物回应信息。在这个过程中，认证机构需分别向持卡人、商家和支付网关发出持卡人证书、商家证书和支付网关证书。三者在传输信息时，要加上发出方的数字签名，并用接收方的公开密钥对信息加密，这样，实现商家无法获得持卡人的信用卡信息，银行无法获得持卡人的购物信息，同时保证商家能收到货款和进行支付。

网上交易的过程看似简单，但却是建立在电子商务基本框架基础之上的。

6.2 电子商务的基本框架结构

电子商务的框架结构是指电子商务活动环境中所涉及的各个领域以及实现电子商务应具备的技术保证。从总体上来看，电子商务框架结构由三个层次和两大支柱构成。其中，电子商务框架结构的三个层次分别是网络层、信息发布与传输层、电子商务服务和应用层；两大支柱是指社会人文性的公共政策和法律规范与自然科技性的技术标准和网络协议。电子商务的框架结构模型如图 6.2 所示。

（1）网络层：网络层指网络基础设施，是实现电子商务的最底层的基础设施，它是信息的传输系统，也是实现电子商务的基本保证。它包括有线电视网、无线通信网、远程通信网和互联网。因为电子商务的主要业务是基于 Internet 的，所以互联网是网络基础设施中最重要的部分。

（2）信息发布与传输层：网络层决定了电子商务信息传输使用的线路，而信息发布与传输层则解决如何在网络上传输信息和传输何种信息的问题。目前 Internet 上最常用的信息发布方式是在 WWW 上用 HTML 语言的形式发布网页，并将 Web 服务器中发

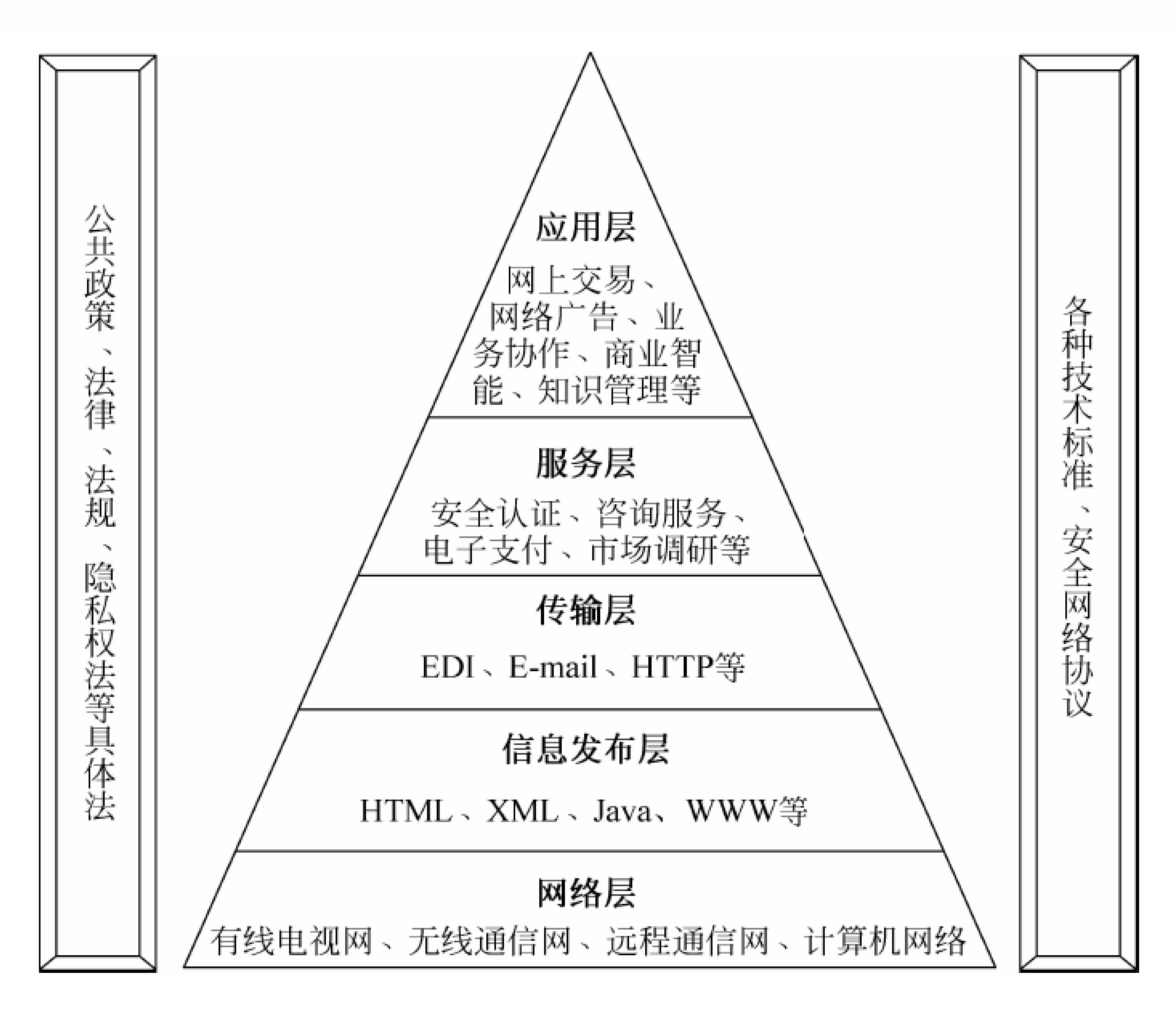


图 6.2　电子商务的框架结构模型

布传输的文本、数据、声音、图像和视频等多媒体信息发送到接收者手中。从技术角度而言，电子商务系统的整个过程就是围绕信息的发布和传输进行的。

(3) 电子商务服务和应用层：电子商务服务层实现标准的网上商务活动服务，如网上广告、网上零售、商品目录服务、电子支付、客户服务、电子认证(CA 认证)、商业信息安全传送等，其真正的核心是 CA 认证。因为电子商务是在网上进行的商务活动，参与交易的商务活动各方互不见面，所以身份的确认与安全通信变得非常重要。CA 认证中心担当着网上“公安局”和“工商局”的角色，而它给参与交易者签发的数字证书就类似于“网上的身份证”，用来确认电子商务活动中各自的身份，并通过加密和解密的方法实现网上安全的信息交换与安全交易。

在基础通信设施、多媒体信息发布、信息传输以及各种相关服务的基础上，人们就可以进行各种实际应用。例如，像供应链管理、企业资源计划、客户关系管理等各种实际信息系统，以及在此基础上开展企业的知识管理、竞争情报活动等。而企业的供应商、经销商、合作伙伴以及消费者、政府部门等参与电子互动的主体也是在这个层面上和企业产生各种互动。

(4) 公共政策和法律规范：法律维系着商务活动的正常运作，对市场的稳定发展起到了很好的制约和规范作用。进行商务活动必须遵守国家的法律、法规和相应的政策，同时还要有道德和伦理规范的自我约束和管理，二者相互融合，才能使商务活动有序进行。

随着电子商务的产生，由此引发的问题和纠纷不断增加，原有的法律、法规已经不能适应新的发展环境，制定新的法律、法规并形成一个成熟、统一的法律体系，成为世界各

国发展电子商务的必然趋势。

(5) 技术标准和网络协议：技术标准定义了用户接口、传输协议、信息发布标准等技术细节。它是信息发布、传递的基础，是网络信息一致性的保证。就整个网络环境来说，标准对于保证兼容性和通用性是十分重要的。

网络协议是计算机网络通信的技术标准，对于处在计算机网络中的两个不同地理位置上的企业来说，要进行通信，必须按照通信双方预先共同约定好的规程进行，这些共同的约定和规程就是网络协议。

6.3 电子商务系统的应用

电子商务系统是由许多系统角色构成的一个大系统。电子商务系统的主要角色有采购者、供应者、支付中心、认证中心、物流中心、电子商务服务商等。电子商务的价值主要体现在与企业结合，特别是与传统企业进行整合，提升企业的竞争能力上。电子商务的实质是企业利用电子方式在客户、供应商和合作伙伴之间，实现在线交易、相互协作和价值交换。除了支持在网上交易中购销的活动外，更强调交易流程的整体效率与效益的提升。商家通过网上交易市场开发新的市场及客户群、维护老顾客、提升供应链效率，从而为企业扩大市场收入、降低运营成本、赢得更高的投资回报创造良好的条件。

然而在电子商务的实际应用过程中，由于各企业的性质和规模存在一定的差异，因此电子商务实现的要求各不相同。就像有的企业是面向消费者的，有的电子商务服务是面向供应商或销售商的，甚至两者兼而有之；在商务活动上有电子采购和在线客户服务等。下面以企业为例，介绍电子商务的应用结构，为电子商务模式分析提供一个整体性的框架，如图 6.3 所示。

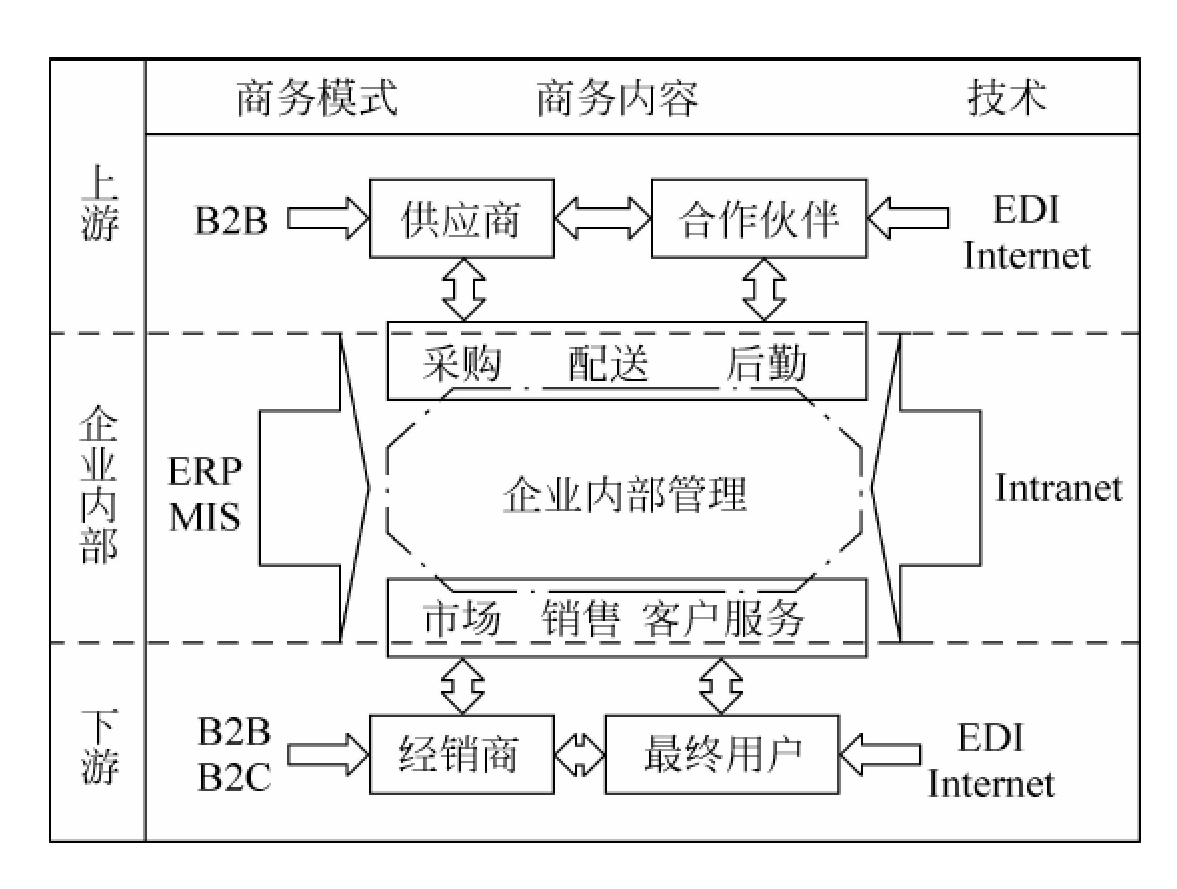


图 6.3 电子商务的应用框架

从图 6.3 中可以看出，首先，电子商务所涉及的对象不但包括供应商、经销商、消费者，而且还包括有关的合作伙伴，如物流公司、银行等，他们共同形成一个完整的供应链。

但对于一个企业来说，其电子商务系统的运作往往只和相邻的上、下游的企业发生业务关系。其次，电子商务系统的业务从材料采购到产品销售和最终售后服务，覆盖范围非常广，包括市场、销售、采购、配送/后勤、客户服务等。最后，电子商务系统的解决方案应该和企业内部的管理系统（如 MIS/ERP）进行集成，只有这样才能真正提升企业的管理效率。

6.4　电子商务的交易模式

电子商务从不同的角度出发，有不同的分类方法，并且由于电子商务的参与者众多，如企业、消费者、政府、接入服务的提供商（ISP）、在线服务的提供者、配送和支付服务的提供机构等，他们的性质各不相同，可分为 B(Business)、C(Customer)、G(Government)，由此形成了以下电子商务交易模式：B2B、B2C、C2C、B2G、C2G 等。目前应用范围比较广泛的是 B2C、B2B、C2C 三大类。

6.4.1　B2C 交易模式

B2C(Business to Customer)电子商务是指企业与消费者之间以 Internet 为主要服务手段进行的商务活动。它是一种电子化零售模式，采用在线销售，以网络手段实现公众消费和提供服务，并保证与其相关的付款方式电子化。它是随着 WWW 的出现而迅速发展起来的，目前在 Internet 上遍布着各种类型的网上商店和虚拟商业中心，提供从鲜花、书籍、饮料、食品、玩具到计算机、汽车等各种消费品和服务。Internet 上有很多这一类型电子商务成功应用的例子，如全球最大的虚拟书店 Amazon.com。为了获得消费者的认同，网上销售商在“网络商店”的布置上往往煞费苦心。网上商品不是摆在货架上，而是做成了电子目录，里面有商品的图片、详细说明书、尺寸和价格信息等。

网上购买引擎和购买指南还不时帮助消费者在众多的商品品牌之间做出选择。消费者对选中的商品只要用鼠标轻轻一点，再把它拖到网络的“购物车”里就可以了。在付款时消费者需要输入自己的姓名、家庭住址以及信用卡号码，一点回车，一次网上购物就算完成。为了消除消费者的不信任感，大多数网上销售商还提供免费电话咨询服务。

1. B2C 在线交易流程

以消费者进行网上购物为例，B2C 交易的过程如下：

(1) 消费者使用自己的计算机，通过互联网搜索想要购买的商品。

(2) 消费者在网上浏览，选购所需的商品放入购物车内，填写系统自动生成的订货单，包括商品名称、数量、单价、总价等，并注明将此商品何时送到何地以及交给何人等详细信息。

(3) 通过服务器与有关商店联系并取得应答，告之消费者所购货物的单价、应付款数、交货等信息。

(4) 消费者确认上述信息后，用电子钱包付款。在系统中装入并打开电子钱包，输入

自己的密码口令，取出其中的电子信用卡进行付款。

(5) 电子信用卡号码被加密发送到相应的银行，网上商店收到订购单，等待银行的付款确认。当然商店不知道、也不应该知道顾客的信用卡信息，无权、也无法处理信用卡中的钱款。

(6) 如果付款不成功，则说明信用卡上的钱款已经超过透支限额或者是上了黑名单，消费者已不能使用该卡。消费者可再次打开电子钱包，取出另一张电子信用卡，重复上述操作。

(7) 如果经银行证明信用卡有效并已授权，网上商店就可付货，同时销售商店留下整个交易过程中发生往来的财务数据，并出示一份电子收据发送给消费者。

(8) 在上述交易成交后，网上商店就按照消费者提供的电子订单，将货物在指定地点交到消费者指明的收货人手中。

就上述电子购物而言，在实际进行过程中，即从顾客输入订货单后开始到拿到销售商店出具的电子收据为止的全过程仅用5～20秒的时间。这种电子购物方式十分省事、省力、省时。购物过程中虽经过信用卡公司和商业银行等多次进行身份确认、银行授权、各种财务数据交换和账务往来等，但所有业务活动都是在极短的时间内完成的。总之，这种购物过程彻底改变了传统的面对面交易和一手交钱一手交货以及面谈等购物方式，是一种新颖有效、保密性好、安全保险、可靠的电子购物过程，利用各种电子商务保密服务系统，就可以在Internet上使用自己的信用卡放心地购买自己所需要的物品。

2. B2C交易商品的特点

B2C电子商务模式最大的特点是商品的交易完全通过网络的方式进行，从消费者在网上挑选和比较商品开始，到网上购物支付和物流配送以及售后服务，是完全以网络为媒介完成的，企业和消费者之间不进行面对面的交易。因此，B2C模式交易的商品有如下特点。

(1) 适合电子传输的产品，如电影、Flash、音乐、电子杂志等，这样的产品被当做B2C电子商务最好的目标产品。

(2) 具有标准化、不易变质、适合传递的产品，如小型数码产品，而非空调、冰箱等大件商品。

(3) 易于搜索的产品，如图书、音乐和光盘等。

随着电子商务的发展，较大的电子商务网站在中心城市周边也设有一定数量的仓库或物流中心，网上销售的商品也日趋丰富，食品、农副产品，甚至汽车等也出现在网上销售的产品目录中。

3. B2C网站实例

亚马逊网上书店(http://www.amazon.com)(图6.4)是国外较成功的B2C网站。亚马逊网上书店的绝大部分顾客都是个人购买者，在书籍和音乐在线零售商间的竞争十分激烈的情况下，由于书籍和音乐都是标准化产品，因此消费者更看重的主要是价格低，送货快、良好的退货政策以及有用的客户服务等。其网上业务主要包括以下几种：



图 6.4　亚马逊网上书店首页

（1）零售。亚马逊书店是世界上最大的在线书店，也是在线书籍市场的领导者。它为超过 150 个国家的 1700 万顾客服务，并出售数百万种商品。为了开拓国际市场，亚马逊网站上建有"International"链接，以方便浏览者访问亚马逊针对非美国消费者的网站（中国版网站是 http://www.joyo.com）。

（2）拍卖。亚马逊在网站上为全球的个人和小企业提供拍卖服务。它采用的是单向拍卖，即只有一个买家或一个卖家，其他人参与竞价。

（3）特色服务。亚马逊的关键特色有方便快捷的浏览和搜索、专家书评、针对个人的购买建议、较低的价格、电子钱包及安全支付系统等。亚马逊网站还提供其他服务以使得在线购物更加有趣。例如，随季节而变的礼品创意与服务、向顾客提供免费的电子动画贺卡等。

（4）客户管理。亚马逊借助其高度自动化的、高效率的后台系统，实现客户关系管理和保持顾客亲密度。当顾客再次访问亚马逊网站时，系统将识别顾客身份，并显示类似"欢迎再次光临，梅里尔"这样的欢迎语，同时根据该顾客以前购买的书籍种类推荐新书。

亚马逊网站跟踪顾客的购物历史，并通过电子邮件寄发购买建议，以吸引回头客。亚马逊还提供详细的产品描述和产品评级以帮助顾客做出购买决定。这些努力带来了令人满意的购物体验，并促使顾客再次访问该网站。

6.4.2　B2B 交易模式

B2B(Business to Business)电子商务是商业对商业，或者说是企业间的电子商务交易模式，即企业与企业之间通过互联网进行产品、服务及信息的交换。目前，世界上 80% 的电子商务交易额是在企业之间，而不是企业和消费者之间完成的。

B2B 电子商务模式包括以下两种基本模式：

（1）面向制造业或面向商业的垂直 B2B。垂直 B2B 可分为两个方向，即上游和下

游。生产商或商业零售商可以与上游的供应商之间形成供货关系；生产商可以与下游的经销商形成销货关系。

(2) 面向中间交易市场的B2B。这种交易模式是水平B2B，它是将各个行业中相近的交易过程集中到一个场所，为企业的采购方和供应方提供了一个交易的机会。B2B只是企业实现电子商务的一个开始，它的应用将会得到不断发展和完善，并适应所有行业的企业的需要。

1. B2B在线交易流程

(1) 采购方向供应方发出交易意向，提出商品报价请求并询问想购买商品的详细信息。

(2) 供应方向采购方回答该商品的报价，并反馈信息。

(3) 采购方向供应方提出商品订购单。

(4) 供应方对采购方提出的商品订购单做出应答，说明有无此商品及目前存货的规格型号、品种、质量等信息。

(5) 采购方根据供应方的应答决定是否对订购单进行调整，并最终做出购买商品信息的决定。

(6) 采购方向供应方提出商品运输要求，明确使用的运输工具和交货地点等信息。

(7) 供应方向采购方发出发货通知，说明所用运输公司的名称，交货的时间、地点，所用的运输设备和包装等信息。

(8) 采购方向供应方发回收货通知。

(9) 交易双方收发汇款通知。采购方发出汇款通知，供应方告之收款信息。

(10) 供应方备货并开出电子发票，采购方收到货物，供应方收到货款，整个B2B交易流程结束。

如果是外贸企业，中间还将涉及海关、商检、国际运输、外汇结算等业务。

2. B2B交易平台上交易商品的特点

B2B交易模式与B2C模式相比较有很多特点，如B2B交易次数少，交易金额大，适合企业与供应商、客户之间大宗货物的交易与买卖活动。另外，B2B模式交易对象广泛，它的交易对象可以是任何一种产品，即中间产品或最终产品。因此，B2B是目前电子商务发展的推动力和主流。

下面以面向中间交易市场的水平B2B为主，介绍交易商品的特点。

(1) 在B2B交易平台上交易的商品覆盖种类齐全。这是因为企业和企业间的交易是大额交易，不像普通消费者以日用、休闲、娱乐等消费品为主，单宗交易、数额小，交易量大。

(2) B2B交易在线下完成，这和企业间的大额交易特点有关。B2B只是一个交易平台，将交易双方汇聚在一起撮合双方的交易。

(3) 交易品的种类不受网络交易的限制。

3. B2B 网站实例

思科连接在线(Cisco Connection On line，CCO，http://www.cisco.com/cn/)(图 6.5)是全球路由器、交换机和其他网络互联设备的领导厂商。从 1991 年开始，思科公司使用增值网提供电子化支持，包括软件下载、故障跟踪和技术建议。1994 年春，思科将服务系统放到网上，并把网站命名为“思科连接在线”。到 2001 年，思科的客户和分销商每月要登录思科网站大约 130 万次以获取技术支持、检查订单或下载软件。在线服务被广泛接受，近 85%的客户服务请求和 95%的软件更新是在线完成的。CCO 被认为是一种成功的 B2B 电子商务模式。下面对其作简要说明。



图 6.5　思科公司首页

(1) 在线订购。思科公司的所有产品几乎都是根据订单生产的，所以没有什么存货。到 1996 年 7 月，通过因特网产品中心，客户服务工程师坐在个人计算机前，在线配置产品，并将订单转给采购部门，然后再以电子化方式提交给思科公司。通过使用在线定价和配置工具，几乎所有的订单(约 98%)都通过 CCO 处理，为思科和它的客户节省了时间。

(2) 查询订单状态。思科的网站每月要接收大约 15 万份订单状态查询请求。公司在国内外的承运商使用 EDI 及时将每次装运的情况用电子化方式输入到思科的数据库中，所有的新信息都能立即提供给顾客。只要已开始装运，思科就通过电子邮件向顾客发出通知。

(3) 思科从 CCO 获得的好处。最重要的好处包括以下几点：

① 降低订单处理费用。通过 1998 年将网上订单处理流程自动化，思科每年节约了

3.63 亿美元。

② 提高技术支持和客户服务效率。通过将 85%的技术支持和客户服务放到网上进行，思科的服务效率每年增加 2.5 倍。

③ 降低费用。1998 年，顾客直接从网站上下载思科最新的软件版本，为公司节约了 1.8 亿美元的复制、包装和发行成本；降低技术支持人员费用约 1.25 亿美元。

④ 交货周期从 4～10 天减少到 2～3 天。

6.4.3 C2C 交易模式

C2C(Customer to Customer)电子商务是消费者对消费者的交易，简单地说就是消费者本身提供服务或产品给消费者。C2C 商务平台就是通过为买卖双方提供一个在线交易平台，使卖方可以主动提供商品上网拍卖，而买方可以自行选择商品进行竞价。

2005 年初以来，中国网民人数剧增，上半年突破 1.03 亿大关，网民访问购物网站的热情进一步提高。经常访问购物网站的网民比例从 2004 年的 16.7%增加到 2005 年的 53.1%，增长了 36.4 个百分点，而同时很少访问购物网站的网民比例下降了 45.9 个百分点。中国个人电子商务市场规模空前增长。

个人电子商务市场的巨大潜力吸引了诸多国内外企业和投资者的眼光，尽管当前中国 C2C 电子商务市场还没有显现任何盈利迹象，但是培育中国个人电子商务市场已经成为国内外众多企业争取用户份额、留住客户、进行强力竞争的手段。

1. C2C 在线交易流程

以交易者网上竞拍为例，C2C 交易流程如下：

(1) 交易者登录 C2C 类型网站，注册相关信息。

(2) 卖方发布拍卖商品的信息，确定起拍价格和竞价幅度、截止日期等信息。

(3) 买方查询商品信息，参与网上竞价过程。

(4) 双方成交，买方付款，卖方交货，完成交易。

2. C2C 交易商品的特点

C2C 交易平台上交易产品丰富、范围广并且以个人消费品为主。因为 C2C 交易本质上也是网上撮合成交通过网上或者网下的方式进行交易。

3. C2C 网站实例

易趣网(http://www.ebay.com.cn/)(图 6.6)是中国著名的电子商务公司，于 1999 年由邵亦波和谭海音合作创办。创业之初，易趣将 C2C 服务作为发展重点，努力打造能促进个人物品交易的平台。目前，易趣网上交易活跃，每 30 秒有新登商品，每 10 秒有人出价，每 60 秒有商品成交。其用户可以通过在线交易平台以竞价和定价形式买卖各式各样的物品。该网站特点如下：



图 6.6 易趣网首页

(1) 易趣不仅是处理闲置物品的平台，网站上出现的新品比例也在不断增加。受消费水平限制，我国二手商品资源缺乏，于是易趣鼓励新品上网交易。随着新品的激增，商品范围也迅速扩张。易趣网站上商品的分类从初期的只有 300 多个细分类发展到 15 大分类，150 多个二级分类，500 多个三级的商品细分类。

(2) 易趣的交易方式随内容而变动。随着商品范围的增加，原有单一的拍卖式交易方式已不能满足需要，易趣推行的定价销售方式受到了用户的欢迎。为满足不同人群的需要，易趣又适时推出了一系列全新的交易方式，包括无底价竞标、有底价竞标、定价出售、一口价成交等几种交易方式。

(3) 易趣的支付方式多种多样。易趣早期采用了邮局汇款、银行卡、手机等支付方式，此后，易趣又推出了“易付通”服务。在卖家和买家交易过程中，买家可以先将钱打入易趣特设的一个账户中，一旦钱到位，易趣会马上通知卖家发货；买家收到货并对货物的数量和质量没有疑义，易趣才会将钱支付给卖家，有效解决了信用风险问题。

(4) 开设企业增值服务。现有增值服务内容包括网上支付、物流配送和短信息服务。其中，网上支付的表现在于易趣与招商银行、广州银联、中国银行、中国农业银行、中国建设银行和中国工商银行等合作，提供网上支付服务。物流配送方面，易趣与 5291.com、快马速递、齐讯速递等物流企业合作，提供面向个人用户的物流解决方案，目前有易付通

和易趣推荐速递两种形式。易趣短信息服务有易趣与中国移动合作共建易趣短信息服务系统，通过订阅短消息，用户可以享受交易提醒、成交通知、买家留言传送等即时功能。

6.5 电子政务

电子政务，在英文中称为 E-Government，简写为 E-Gov。电子政务是政府部门运用先进的电子信息技术手段(计算机、网络、电话、手机、数字电视等)，以实现政务信息数字化、政务公开化、办公高效化、服务网络化等为目标，将管理和服务通过网络技术进行集成，向社会提供优质和全方位的、规范而透明的、符合国际标准的管理和服务的过程。电子政务是在吸取了电子商务的经验基础上发展起来的基于 Internet 的应用。

实验 10 注册与基础实践

一、实验目的

利用软件来学习掌握电子商务的基本交易实践活动。

二、实验原理

电子商务就是利用电子数据交换(Electronic Data Interchange，EDI)、电子邮件、电子资金转账(Electronic Financing Turn，EFT)及 Internet 的主要技术在个人间、企业间和国家间进行无纸化的业务信息的交换。

EDI 标准是由各企业、各地区代表共同讨论、制订的电子数据交换共同标准，可以使各组织之间的不同文件格式通过共同的标准，获得彼此之间文件交换的目的。EDI 标准具有足够的灵活性，可以适应不同行业的不同需求，但由于每个公司都有其自己所规定的信息格式，因此当发送 EDI 电文时，必须将公司内部数据翻译成 EDI 的标准格式进行传输。

三、实验背景

李明以及他的企业“南京奥派科技”都将需要学习利用电子商务。李明要给王军和张玲转账，首先他要给自己注册一个个人银行账户，并进行存款。南京奥派科技与南京舜天科技素有生意往来，要利用电子商务，就需要在网上银行开通企业付款通道。

四、实验内容

实验开始前，先要进行个人信息和企业信息的维护，网上银行参数设置。

提示：

李明和王军申请工商银行的账户，张玲申请招商银行的账户；南京奥派科技和南京舜天科技各在工商银行注册一个企业账户。

五、实验步骤

1. 基础信息设置

(1) 按照图 6.7 输入学生用户名和密码，单击“登录”按钮。登录后可以看到教师为该学生制定的实验列表，单击“进入”按钮，即可进入该实验。



图 6.7　用户登录

（2）为该实验创建空间：单击“我也要建实验空间”标签，开始创建空间，如图 6.8 所示。输入空间名称，并选择空间类型、实验类型，单击“创建”按钮，然后单击空间后的“进入”按钮，开始实验。



图 6.8　创建空间

2. 申请个人账户

（1）选择“电子支付实践”模块，可见该模块下有两部分，分别为“网上银行”和“支付通”，如图 6.9 所示。李明要申请他在工商银行的个人账户，首先就要选择“中国工商银行”选项，单击“个人账户申请”超链接。

（2）填写注册信息，然后单击下方的“申请”按钮，如图 6.10 所示。

（3）单击右下角的“切换用户”，进入“银行柜台”（参见图 6.9），对申请的账户进行审批，如图 6.11 所示。单击操作下方的“审批”按钮，审批通过，李明的这个账户申请成功。

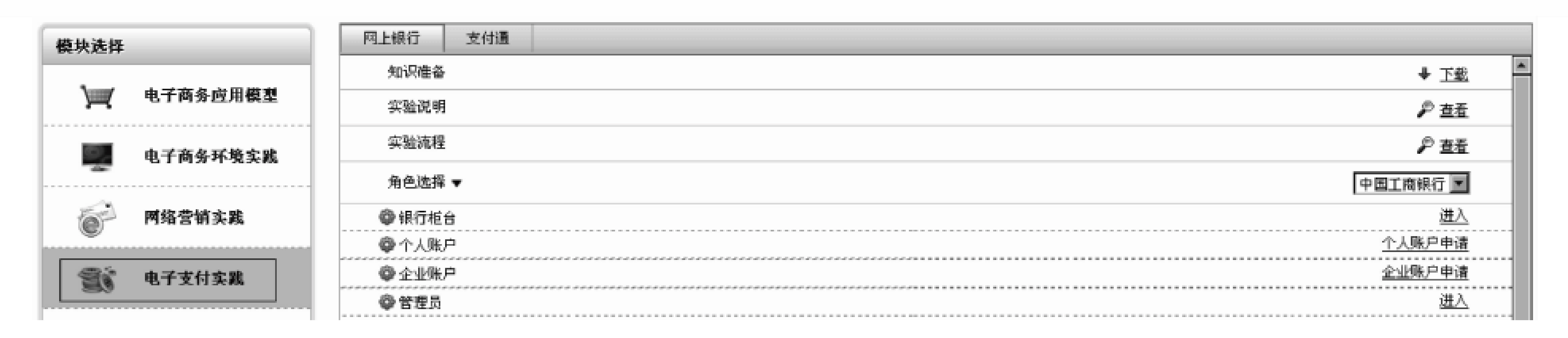


图 6.9　电子支付实践



图 6.10　填写注册信息

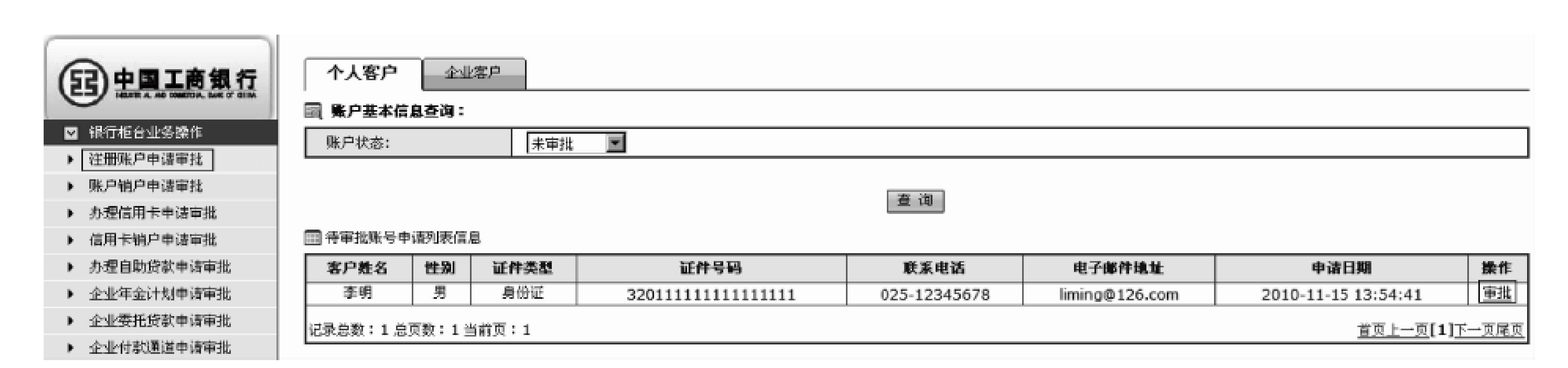


图 6.11　审核账户申请

(4) 按照以上步骤,在工商银行申请王军的个人账户,在招商银行申请张玲的个人账户。申请的时候要注意,系统默认的是李明的资料,需要把相关信息改过来。另外,在招商银行申请账户时,需要在“角色选择”下拉列表框中选择相应的银行。

3. 申请企业账户

(1) 单击“企业账户申请”超链接(参见图 6.9),按照申请要求,填写申请表,如图 6.12 所示。填写完成后,单击表格下方的“申请”按钮,等待银行柜台审核。

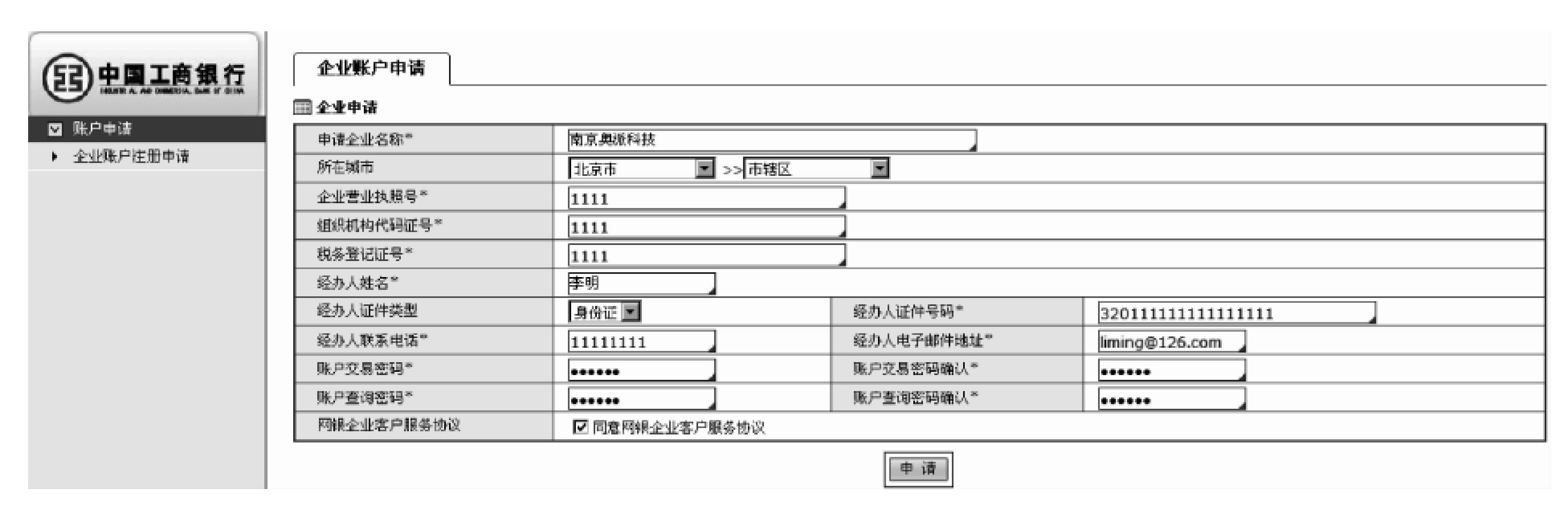


图 6.12　企业账户申请

（2）单击“银行柜台”右侧的“进入”超链接(参见图 6.9)。在“注册账户申请审批”中选择“企业客户”选项卡,如图 6.13 所示。单击操作下方的“审批”按钮,审批通过,账户申请成功。

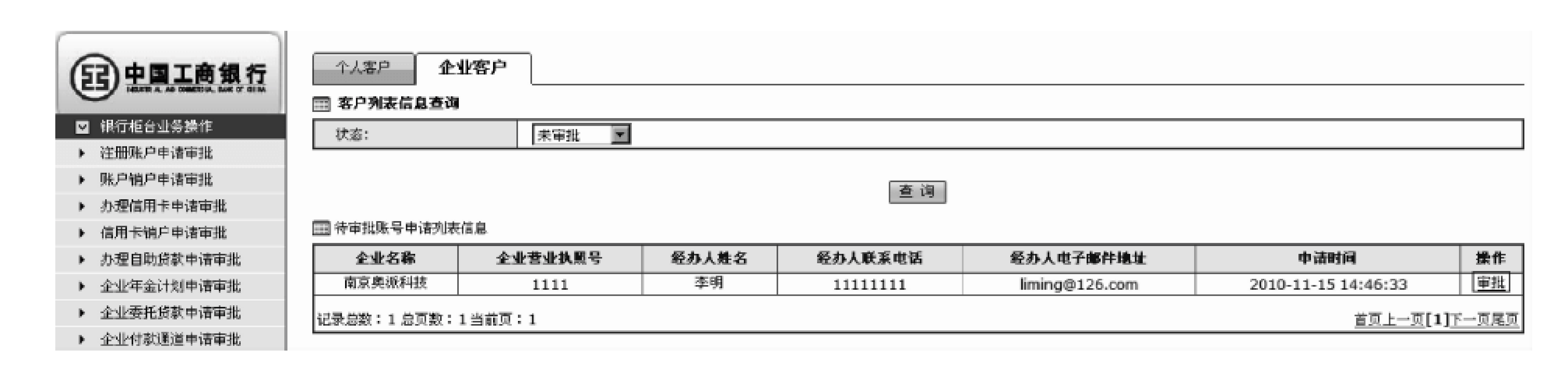


图 6.13　企业账户审核

（3）按照以上步骤,申请南京舜天科技的银行账户。

4. 网上银行支付初步

1）个人银行存款

李明要在自己的账户中存入 10 万元。

（1）在“李明”的右侧单击“进入银行柜台”超链接,如图 6.14 所示。



图 6.14　进入银行柜台

（2）在存款金额中填入所要存入的金额(100 000),然后单击“确定存款”按钮,如图 6.15 所示。

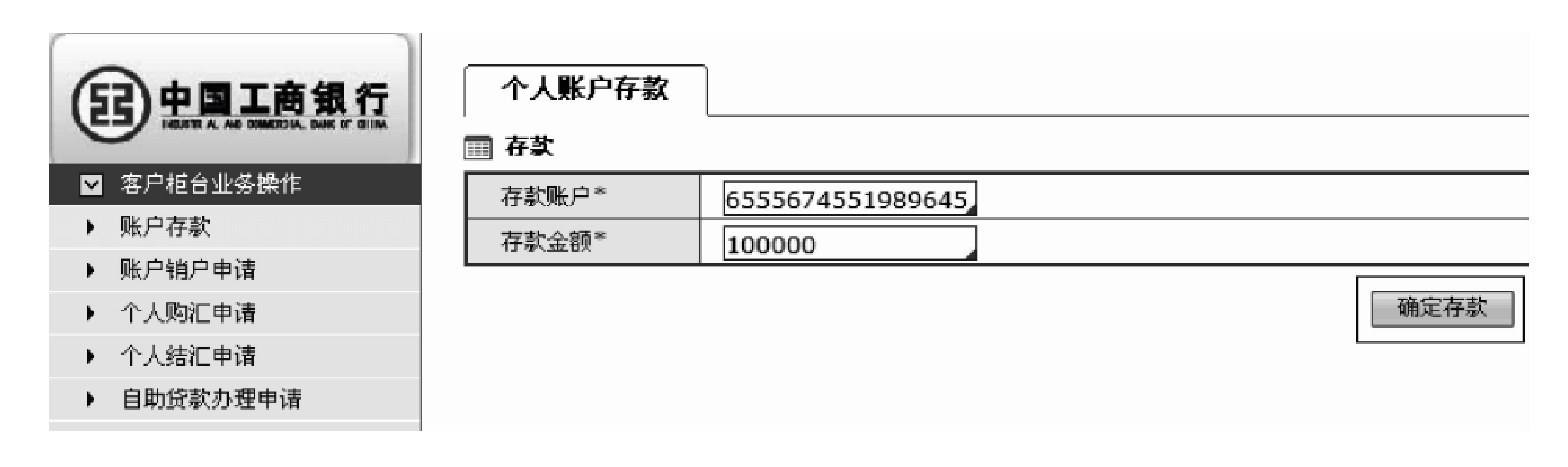


图 6.15　输入存款

（3）按照以上步骤,为王军、张玲各存入 1000 元。

2）个人银行转账

（1）同行转账：李明要给同在工商银行开户的王军打 1000 块钱,进入个人网上银行,单击“进入银行柜台”超链接,如图 6.16 所示。



图 6.16 进入银行柜台

（2）在左侧的“转账汇款”中选择“同行转账”选项，按要求填好汇款单，如图 6.17 所示。



图 6.17 填写汇款单

（3）单击“提交”按钮，再输入交易密码，如图 6.18 所示。单击“确定”按钮，此次转账就成功了。

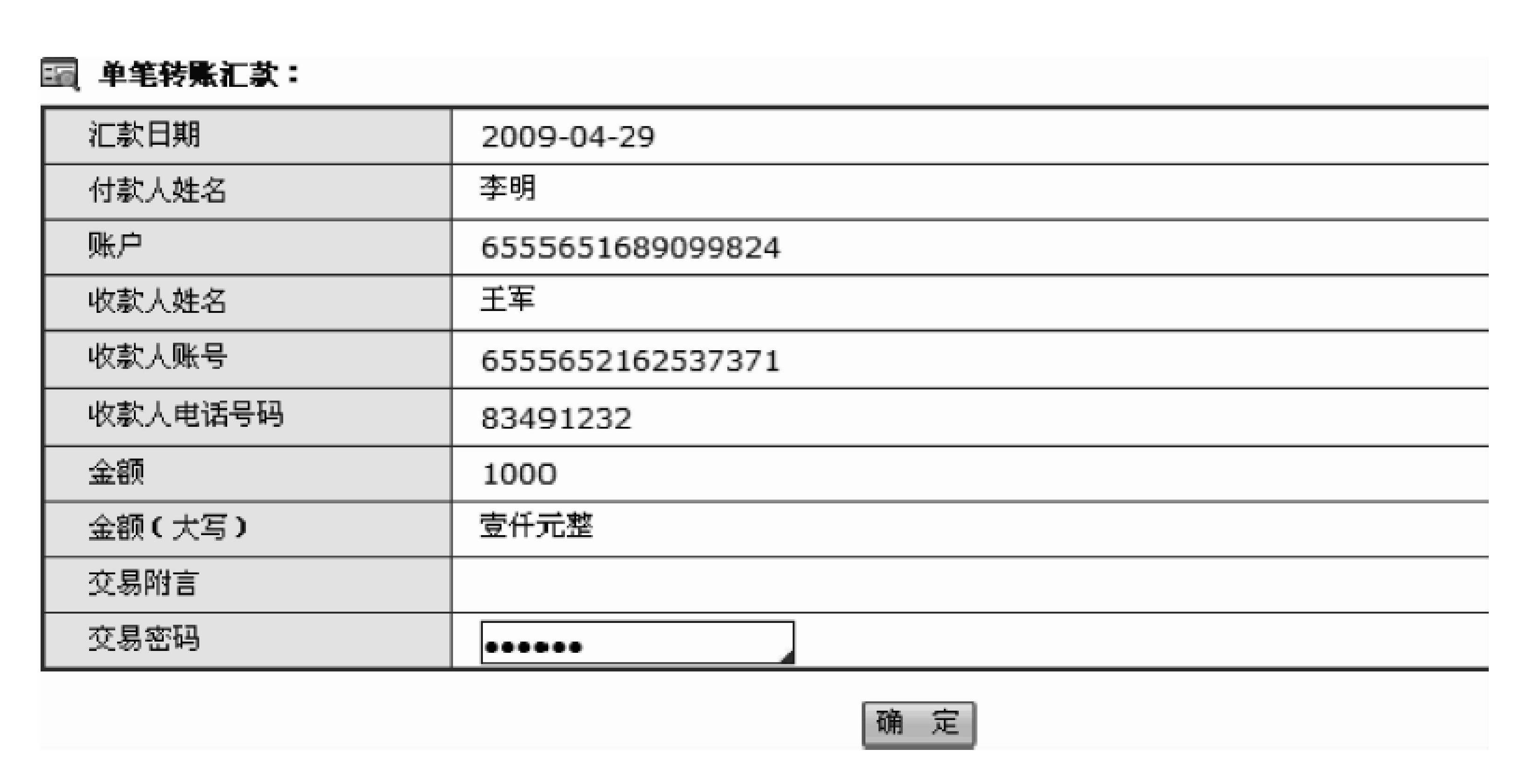


图 6.18 填写交易密码

（4）跨行转账：张玲的开户银行是招商银行，她也可以接受在工商银行开户的李明汇款。在“转账汇款”中选择“跨行转账”选项，按要求填好汇款单，如图 6.19 所示。

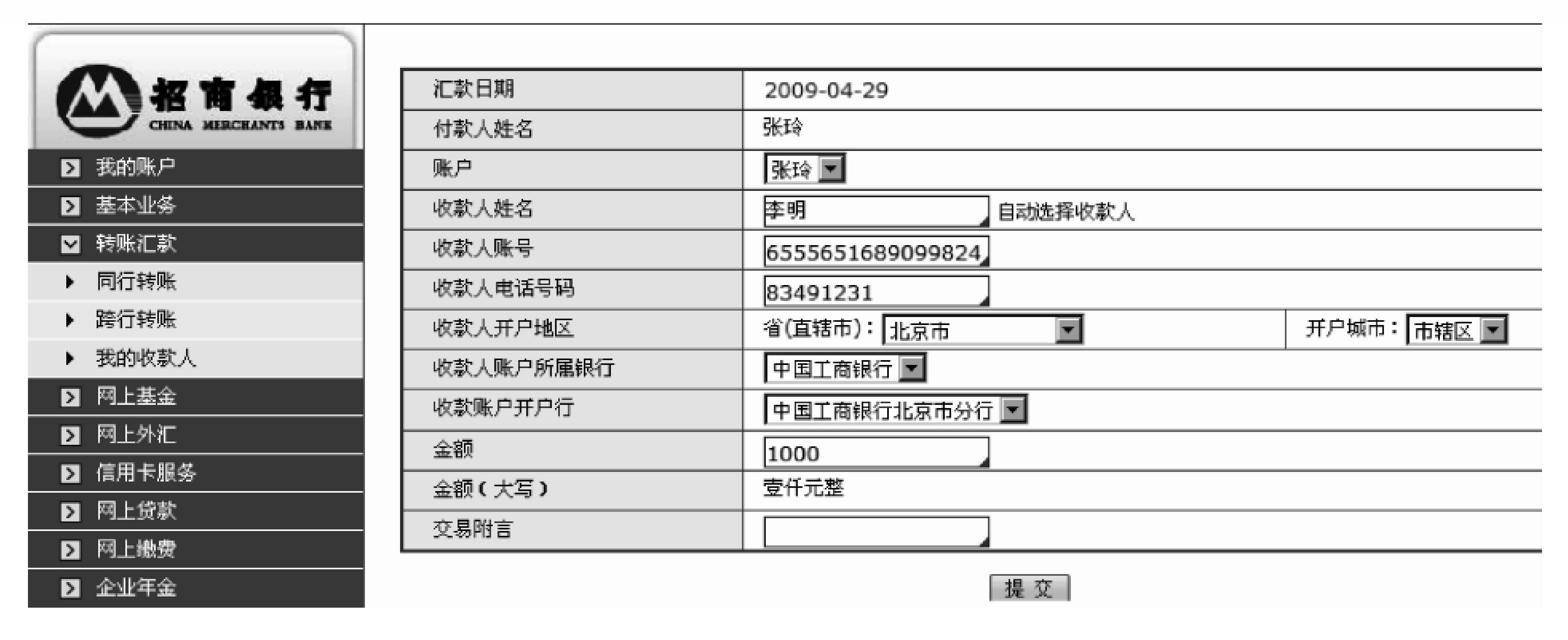


图 6.19　跨行转账

(5) 单击“提交”按钮，再输入交易密码，如图 6.20 所示。单击“确定”按钮，此次转账就成功了。



图 6.20　输入交易密码

3) 企业银行存款

当企业银行账户申请成功之后，会收到新邮件，告诉你账户的用户名和密码，这在以后的操作中是要用到的。

(1) 单击计算机桌面右下角的 按钮，注意不同的企业对应不同的账号。单击“邮件主题”，查看邮件内容，如图 6.21 所示。需要记住账户的用户名和密码，在登录企业网上银行的时候需要用到。



图 6.21　邮件内容

(2) 单击“进入银行柜台”超链接,输入存款金额,如图 6.22 所示。单击“确定存款”按钮,即操作成功。



图 6.22　输入存款金额

5. 企业账户开通付款通道

(1) 单击“进入银行柜台”超链接,进入南京奥派科技的企业银行柜台,在界面的左边选择“企业付款通道申请”选项,填写申请表,如图 6.23 所示。其中的“实时反馈 URL”是指网页地址,是因特网上标准资源的地址。填写完成后,单击“申请”按钮,等待银行审批。



图 6.23　企业付款通道申请

(2) 切换用户,进入“银行柜台”,选择“企业付款通道申请审批”选项,单击“审批”按钮,进行审批,然后单击“审批通过”按钮,如图 6.24 所示。



图 6.24　审批通过

6. 支付通初步

给支付通的服务商绑定银行账户。李明需要在支付通网站申请账户，并通过网上银行进行充值，支付通账户里面的钱也可以用来提现。由于在电子商务应用模型B2B、B2C及C2C中的服务商要设置支付通账号，李明在申请支付通账号之后，还必须开通一下商家服务，才会有商号和密钥，商号和密钥在服务商绑定支付通账号时会用到。

1）开通支付通账户

（1）在“电子支付实践”模块中单击“支付通”，在“支付通”选项卡的“服务商平台”右侧单击“进入”按钮，为服务商绑定一个银行账号。这样，支付通的用户才能使用支付通。在“银行账户管理”中单击“新增账户”按钮，如图6.25所示。

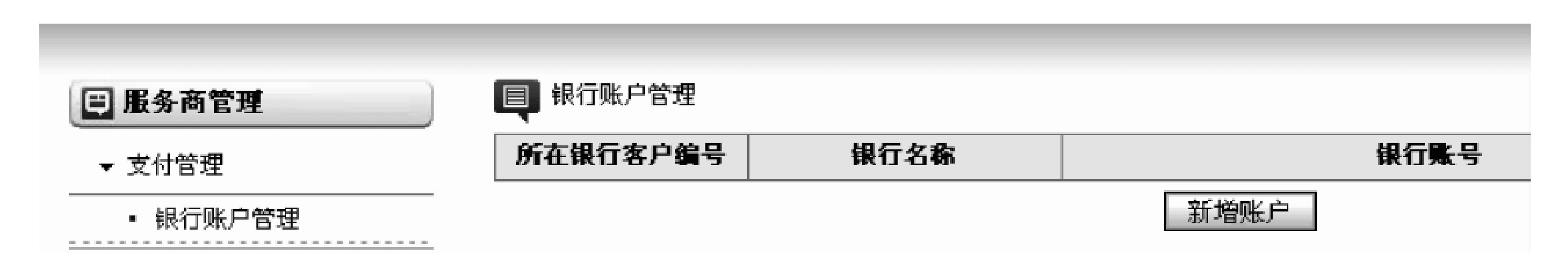


图6.25　新增账户

（2）填写账户信息，银行商户编号在登录企业网上银行时可以看到。填写完成后单击“添加银行账户”按钮，这样，服务商就成功绑定银行账户了，如图6.26所示。

银行账户管理

银行名称：	中国工商银行
所在银行商户编号：[*]	6
企业名称：[*]	南京奥派科技
银行帐号：[*]	6555671014695822

注：输入的银行账户需开通企业付款通道功能。 如何开通企业付款通道功能？

添加银行账户

图6.26　新增账户信息

（3）单击“支付通平台”后面的“进入”按钮。注册支付通账户有两种方法：可以使用手机注册，也可以使用邮箱注册。这里李明以个人身份，选择用手机注册。在弹出的界面中输入手机号码和校验码，单击“同意并确认注册”按钮，如图6.27所示。

第1步：填写账户名

请填写您的常用手机号码.

*手机号码：13911111111　检查账户名是否可用

我们将向此号码发送确认信息，请仔细核对填写的手机号码是否正确

4866D　4866D　请输入左侧图片中的校验码。

同意并确认注册

图6.27　填写手机注册信息

(4) 这时,注册手机会收到一条包含校验码的短信。单击界面右下方的 <1> 按钮,查看校验码,如图 6.28 所示。



图 6.28　手机注册

(5) 在弹出的界面中,输入校验码,单击"下一步"按钮。然后填写相关信息,单击"同意以下条款,并确认注册"按钮,如图 6.29 所示。这样,李明就成功注册了他的支付通账户。

用邮箱注册账户的方法相似。

注意:使用邮箱注册的支付通账户需要进入邮箱进行激活。进入右下角的邮箱,阅读邮件,单击激活链接即可。

2) 支付通账户充值以及提现

(1) 充值:李明要使用支付通,他的账户里面就需要充值,以方便在以后的电子商务实践中付款。进入李明个人的支付通账户,在"我的支付通"中选择"充值"选项,如图 6.30 所示。李明是要给自己的账户充值,而他的开户银行是工商银行,所以选择"中国工商银行",充值 10 000 元。输入充值金额,单击"下一步"按钮。

(2) 单击"去网上银行充值"按钮,在出现充值的订单中,按要求输入自己的银行账号和密码,以及附加码,单击"确定"按钮。充值成功后,系统给出提示,表示李明成功地给自己的支付通账户充值了 10 000 元。

(3) 提现:支付通提现的金额是打到绑定的银行账户中的。同充值操作一样,只是在"我的支付通"中改选"提现"选项。申请提现,首先是要设置银行账号,如图 6.31 所示。

(4) 输入支付密码。

注意:该支付密码是指支付通账户的支付密码,而非银行账号的密码。

支付通

您好，请 注册 或 登录

通过Email地址，您可以安全、简单、快捷的进行网上付款和收款。

1、您的账户名

账户名：13911111111

2、设置登录密码

*登录密码：●●●●●●●●　为了您的账户安全，请牢记您的登录密码。

*确认登录密码：●●●●●●●●

3、设置支付密码

*支付密码：●●●●●●●●●　为了您的账户安全，请牢记您的支付密码。

*确认支付密码：●●●●●●●●●

4、设置安全保护问题

*安全保护问题：1

*您的答案：1

5、填写您的个人信息（请如实填写，否则将无法正常收款或付款）

用户类型：（信息提交后将无法修改）

⊙个人

以个人姓名开设支付通账户。

○ 公司

以营业执照上的公司名称开设支付通账户。开设此类账户必须拥有公司类型的银行账户。

*真实名字：李明

证件类型：身份证

*证件号码：320111111111111111

*手机号码：13911111111

联系电话：

同意以下条款，并确认注册

图 6.29　填写相关信息

（5）输入以李明本人的名字开户的银行账号，这点是需要注意的，否则提现存在风险。填写完毕，单击“保存银行账户信息”按钮，如图 6.32 所示。

（6）设置好银行账号后，选择“申请提现”选项卡，输入提现金额以及支付通账户的支付密码，单击“下一步”按钮，如图 6.33 所示。

（7）确认提现银行信息正确无误后，单击“确定提现”按钮。这样，系统就会提示“提现申请成功”。

（8）按照上述的步骤，李明、王军和张玲再用邮箱申请两个支付通账号。其中李明用手机申请的账户用于 B2B、B2C、C2C 以及网络广告交易市场中的服务商。



图 6.30 向支付通内充值



图 6.31 提现



图 6.32 输入个人信息



图 6.33　设定支付密码

下面以李明刚才申请的支付通账号为例，开通一下商家服务。

（1）进入李明的支付通账户，单击"商家服务"标签，选中"网站集成 ZFT"选项，单击"点此申请"按钮。然后填写申请信息，单击"下一步"按钮，如图 6.34 所示。在弹出的对话框中，单击"同意协议并付款"按钮。



图 6.34　填写申请信息

(2) 申请了之后需要支付通的服务商审批一下。切换用户,进入服务商平台,在“商户管理”中开通商家服务功能,单击“确认付费,开通功能”按钮。

(3) 回到李明的支付通账户,再次选择“商家服务”选项卡,可以看到一个交易安全校验码和合作者身份。这两个号码是需要备份的,在 B2B、B2C、C2C 以及网络广告交易市场实验中将会用到。

7. 思考题

怎么实现支付通的充值?



第7章

电子商务环境搭建与营销支付篇

7.1 引言

随着电子商务的蓬勃发展，网上商店对于网民来说已经不再是一个陌生的字眼，大多数网民张口便能说出一大串购物网站的名称，诸如 8848 网站和易趣、淘宝网等，还有新浪、搜狐的网上商城，亚马逊、卓越、当当等网上超市，各购物网站所销售的商品既有保健品、日用品、书籍、音像制品、文具等小商品，也有音响、照相机、手机、洗衣机等大件商品。

电子商务营销是网上营销的一种，是借助于因特网完成一系列营销环节，达到营销目标的过程。我们知道，网络具有快速、高效、低成本的特点，在因特网上信息资源共享，进入障碍为零。作为一种新的媒体，网络具有一对一的互动特性，这是对传统媒体面对大量"受众"特征的突破。从营销的角度讲，网络上生产者和消费者一对一的互动沟通，了解顾客的要求、愿望及改进意见，将工业时代大规模生产、大规模营销改进为小群体甚至个体营销，为消费者提供了极大的满足，迎合了现代营销观念的宗旨。

7.2 电子商务的环境

同自然界的其他任何系统一样，电子商务系统的顺畅运行也有其赖以生存的支撑环境，主要包括电子商务的支付环境、物流环境和信用环境等。

7.2.1 电子商务的支付环境

随着网上电子交易业务量的增加，支付问题日益突出，如何处理不同范围内的大宗交易，成为电子商务活动的关键，而答案是唯一的，即利用电子支付。

电子支付是电子商务活动的关键环节，是电子商务能够顺利发展的基础条件。对于商家来说，如果缺乏良好的网上电子支付环境，电子商务高效率、低成本的优势就难以发挥，只能是网上订货、网下支付，实现的是较低层次的商务应用，从而使电子商务的应用与发展受到极大的阻碍。因此，提供安全、高效、快捷的网上金融服务就成为整个电子商务交易过程中最重要的环节。

但由于电子支付是通过开放的 Internet 来实现的，支付信息很容易受到黑客的攻击和破坏，这些信息的泄露和受损直接威胁到企业和用户的切身利益，所以安全性一直是电子支付实现所要考虑的最重要的问题之一。

7.2.2 电子商务的物流环境

随着电子商务时代的到来，企业销售范围不断扩大，企业和商业销售方式及最终消费者购买方式的转变，使得送货上门等业务成为一项极为重要的服务业务，这些极大地促进了物流行业的兴起。

物流是指物质实体（商品或服务）的流动过程，具体指运输、储存、配送、装卸、保管、物流信息管理等各种活动。对于少数商品和服务来说，可以直接通过网络传输的方式进行配送，如各种电子出版物、信息咨询服务、有价信息软件等。而对于大多数商品和服务来说物流仍要经由物理方式传输，但由于一系列机械化、自动化工具的应用，准确、及时的物流信息对物流过程的监控，将使物流的速度加快、准确率提高，能有效地减少库存，缩短生产周期。

在这一发展过程中，物流不仅已成为有形商品网上商务的一个障碍，而且也已成为有形商品网上商务活动能否顺利进行和发展的一个关键因素。因为电子商务优势的发挥需要有一个与电子商务相适应的，高效、合理、畅通的物流系统，否则电子商务就难以得到有效的发展。

7.2.3 电子商务的信用环境

传统商务和电子商务的运作过程中，商贸交易过程的实务操作步骤是相同的，但交易具体使用的运作方法是不同的。在电子商务条件下，商务活动是通过网络进行的，买卖双方在网上沟通，签订电子合同、使用数字签名和电子支付等，这完全改变了传统商务模式下面对面的交易方式，因此商业信用体系的建立对电子商务来说就显得更加重要。它不是仅依靠交易双方单方面的努力就能解决的，电子商务信用环境的建立是一个综合性的任务，这当中既有公民道德素质的提高和意识觉醒问题，也有技术问题和法律问题，同时信用环境的建立还有待时间让电子商务系统各个角色逐渐习惯和适应。要解决这些问题，首先，需要社会各方面的大力引导，创建一个具有良好信用意识的社会环境；其次，建立和完善电子商务认证中心，这是改善电子商务信用环境最基本的技术手段，是电子商务活动正常进行的必要保障；再次，制定相关法律和制度，规范电子商务的交易行为，保障电子商务活动的正常进行；最后，建立社会信用评价制度和体系，为电子商务交

易提供资信服务。

电子商务系统的支撑环境除了以上提到的三种之外，还和许多因素有关，如计算机的普及程度和上网率、企业领导对电子商务运作的重视程度及职工素质等。2005年国家发改委开展了电子商务支撑环境项目试点工作，目的是进一步推动骨干企业电子商务建设，鼓励骨干企业优化业务流程和组织结构。

7.3　电子商务环境下的新型网络营销

7.3.1　网络营销优势

1. 企业对顾客需求反应能力提高

企业通过电子商务平台拓展对顾客需求的反应方式和途径。传统反应方式多以事后回应为主，即等顾客需求真实发生并将信息传递到公司总部后，市场部才做出回应，相关措施再按原信息流逆向传递，层层分派。速度慢，限制了企业对顾客需求的反应能力。电子商务为企业提供了更宽泛的服务平台，在顾客与企业间构建出广泛的沟通渠道。企业可以通过前期的信息收集和数据分析，直接将产品和服务信息提前传递给顾客；通过引导消费的方式，先于顾客发现需求；通过设立网上商店，记录顾客消费和需求信息；开通网络论坛，提供在线服务等多种互动方式，将过去的被动回应改为主动响应，持续向全球顾客提供高质量产品和服务，提高了对顾客需求的反应速度和效率。

2. 企业与顾客关系更密切

网络强大的通信能力和电子商务系统便利的商品交易环境，缩短了企业与消费者之间的实际距离，促使营销者和消费者的沟通方式发生变化，消费者可以亲自参与到产品设计、生产、评测环节中，成为企业经营全过程中重要的、积极的参与者。网络环境下，通过电子商务手段，企业将信息以多媒体方式在网上传播，并以智能搜索和查询的方式，方便消费者主动在网络上搜索，消费者可以了解更多商品与服务信息，企业直接面对消费者，和消费者进行沟通交流，共同创造新的市场需求。麦当劳曾在上海1个月共发出15万条手机短信，短信只针对目标客户，在正确的地方、合适的时间场合，效果非常好，对这种短信促销的回应率有12％，比之传统直接促销手段（回应率只有1％～5％）有很大提高。这是麦当劳最有效、最成功的营销活动之一，为其获得了新的消费者。

3. 企业的竞争优势增加

网络营销能够将产品说明、促销、顾客意见调查、广告、公共关系、顾客服务等各种营销活动整合，进行一对一沟通，不受地域限制，结合文字、声音、影像、图片及视讯，用动态方式展现，并能轻易迅速地更新资料，同时消费者也可重复上线浏览查询。结合问卷、网络、资料库，以最新、最快、最详尽的方式获得顾客信息，通过网络互动的资料修订与智慧型的统计分析功能，掌握大量主要顾客与潜在顾客的完整资料。综合这些功能，相当于创造了无数的经销商与业务代表，不需付房租，不需付薪水，节省了营销渠道成本，使企

业获得低成本的竞争优势。

7.3.2 网络营销策略

网络营销策略包括以下几种：

(1) 扩大产品线规模。不局限于主要产品，而依据拥有的资料，主动分析消费需求与欲望，开发多种类型产品，增加购买规模。

(2) 强化顾客关系。加强与顾客的双向互动，分析顾客资料，设法掌握更多顾客特性，开发出更多产品适应顾客需求。

(3) 营销渠道多元化。将传统营销与包括网络等新型渠道紧密结合，以建立最大的顾客接触，扩大市场占有率。

(4) 消费需求准确化。分析归纳顾客资料，更准确地定位目标市场，做出有效的市场促销。再利用多彩的网络多媒体功能，给新上网的顾客留下深刻印象，增加市场顾客规模，扩大网络营销效益。

7.3.3 电子商务营销中的4C

当前，第三产业中服务业的发展是主要经济增长点，新型服务业如金融、通信、交通等产业如日中天。社会要求企业发展必须以服务为主，以顾客为中心，为顾客提供适时、适地、适情的服务，最大程度上满足顾客需求。互联网络作为跨时空传输的“超导体”媒体，可为顾客提供及时服务，同时网络的交互性可以了解顾客需求，提供针对性响应，利用互联网络，传统4P(产品/服务、价格、分销、促销)营销组合可以更好地与以顾客为中心的4C(顾客、成本、方便、沟通)相结合。

1. 产品和服务以顾客为中心

互联网络起源于1969年，美国西海岸四所大学和研究所将主计算机以50Kbps的线路连接起来，架设了一个小型通信网络，称为ARPANET。到了1974年，ARPANET已拥有100个结点的网络，再成长形成今天的数以百万计网点规模的全球互联网络。

由于互联网络具有很好的互动性和引导性，用户通过互联网络在企业的引导下对产品或服务进行选择或提出具体要求，企业可以根据顾客的选择和要求及时生产并提供及时服务，使得顾客跨时空得到满足要求的产品和服务；另一方面，企业还可以及时了解顾客需求，根据顾客要求组织生产和销售，提高企业生产效益和营销效率。

2. 以顾客能接受的成本定价

传统的以生产成本为基准的定价在现代市场营销中必将被摈弃，新型价格以顾客能接受的成本定价，依据该成本组织生产和销售。企业以顾客为中心定价，测定市场中顾客的需求及对价格认同的标准，顾客通过互联网提出接受的成本，企业根据顾客的成本提供柔性的产品设计和生产方案供用户选择，直到顾客认同后再组织生产和销售，所有这一切都是顾客在公司的服务器程序导引下完成，不需要专门的服务人员，成本极低廉。例如，美国通用汽车公司允许顾客在互联网上通过公司的有关导引系统，自己设计和组

装满足需要的汽车，用户首先确定接受的价格标准，系统根据价格限定显示满足要求样式的汽车，用户可以适当修改，公司最终生产的产品恰能满足顾客对价格和性能的要求。

3. 压迫式促销转向加强与顾客的联系沟通

传统促销是企业为主体，通过一定的媒体或工具对顾客进行压迫式的销售，以加强顾客对公司和产品的接受度和忠诚度，顾客是被动接受的，缺乏沟通和联系，公司促销成本很高。互联网络上营销是一对一和交互式的，顾客可以参与到公司的营销活动中，互联网更能加强与顾客的沟通和联系，更了解顾客需求，更易引起顾客认同。例如，美国的雅虎（Yahoo）公司开发了能在互联网络上对信息分类检索的工具，由于该产品具有很强的交互性，用户可以将自己认为重要的分类信息提供给雅虎公司，雅虎公司马上将该分类信息加入产品中供其他用户使用，不用宣传其产品就广为人知，短短两年公司股票市场价值增长几百倍。

4. 企业可实现低成本跨国营销

在经济全球化条件下，企业要获得全球优势，必须在全球范围内配置资源，充分考虑成本、自然资源、法律、竞争、销售等多种影响基础上，做出科学的营销决策，占领国际、国内两个市场。特别是实力雄厚的跨国公司，早已把全球市场置于自己的营销范围内，以一种全球营销观念来指导公司的营销活动。例如，可口可乐公司在世界几十个国家布有生产据点，100多个国家拥有市场，成为一个总部设在美国的全球公司。电子商务的应用使企业能够在短时间内对收集到的信息进行横向比较和纵向分析，实现企业全球资源低成本调配整合。“遍布全球的互联网络为跨国公司在全球范围内传播和提高品牌形象创造了优越的技术条件。在互联网上做广告可以在瞬间以极低的运营成本和直通个人的特点将品牌信息准确无误地发送给事先设计好的群体，这无疑可以增强全球客户的品牌认知和偏好，使品牌形象信息能够以最快的速度在最大的范围内得以传播。”这种品牌传播的有效性有利于提高企业美誉度，获得品牌忠诚。总之，随着全球经济一体化进程加快，计算机、通信、网络等技术广泛应用，人类社会将从过去工业经济时代进入到电子商务时代。电子商务代表未来商务发展方向，也代表了网络时代新型企业营销模式。不仅使企业营销成本降低，增强企业的核心竞争力，使之立于不败之地，更重要的是使广大消费者受益。未来是信息世纪、网络世纪，人员营销、广告促销、经销代理等传统营销手法将与网络营销相结合，形成以最低成本投入获得最大市场量的新型营销模式。

7.4　电子支付

7.4.1　电子商务与网上支付的关系

电子商务是指通过计算机和网络来完成商品的交易、结算等一系列商业活动过程的一种方式，其内容包括信息流、资金流和物流。信息流和资金流直接以因特网为基础，应该说信息流和物流比较容易实现，而资金流即网上支付实现起来却比较复杂，所以人们

在谈及电子商务时，往往把网上支付手段作为衡量是否真正实现电子商务的标志。电子商务其核心问题是如何确保网络交易中的电子支付的有效性和安全性。网上支付是指以计算机及网络为手段，将负载有特定信息的电子数据取代传统的支付工具用于资金流转，并具有实时支付效力的支付方式。网上支付作为新的网络交易支付方式，它的应用和发展给传统支付模式带来了很大的冲击和挑战。

当分析这种支付模式的特征时，不难发现由事物本质属性影射出其潜藏的不安全因素。网上支付是采用先进的技术通过数字流转来完成信息传输的，其各种支付方式都是采用数字化的方式进行款项支付的，于是人们就开始质疑信息数字化后数据传输过程中信息丢失、重复、错序、篡改等安全性问题；网上支付的工作环境是基于一个开放的系统平台之中，交易双方的身份置于虚拟世界中，这无疑增加了电子支付的风险；网上支付使用的是最先进的通信手段，对软、硬件设施的要求很高，技术软件不成熟就为黑客等不法分子提供了可乘之机，所以，研制出一套无懈可击的互联网支付系统成为制约电子商务发展的瓶颈。

7.4.2 我国网上支付的工具

我国网上支付的工具有以下几种：

(1) 银行卡在线转账支付。银行卡在线转账支付是目前我国应用非常普遍的电子支付模式，付款人可以使用申请了在线转账功能的银行转账小金额资金到收款人的银行账户中。

(2) 电子现金。电子现金是以数据形式存在的现金货币。它把现金数值转化为一系列的加密序列数，来表示现实中各种金额的币值。

(3) 第三方支付平台。这种形式的支付过程是买家在网上把钱付给支付宝公司，支付宝收到货款之后通知卖家发货，买家收到货物之后再通知支付宝，支付宝这时才把钱转到卖家的账户上。此平台是我国现在比较成熟的电子商务交易平台。

7.4.3 电子支付安全协议

如何通过电子支付安全地完成整个交易过程，又是人们在选择网上交易时所必须面对的、而且是首先要考虑的问题。就目前而言，虽然电子支付安全问题还没有形成一个公认的、成熟的解决办法，但人们还是不断通过各种途径进行大量探索，SSL 安全协议和 SET 安全协议就是这种探索的两个重要结果，它们已经广泛在国际间的电子支付中使用。

1. SSL 安全协议

SSL 安全协议最初是由 NetscapeCommunication 公司设计开发的，又称为安全套接层(Secure Sockets Layer)协议，主要用于提高应用程序之间的数据的安全系数。SSL 协议的整个概念可以被总结为：一个保证任何安装了安全套接字的客户和服务器间事务安全的协议，它涉及了所有 TCP/IP 应用程序。在电子商务交易过程中，由于有银行参

与，按照 SSL 协议，客户购买的信息首先发往商家，商家再将信息转发银行，银行验证客户信息的合法性后，通知商家付款成功，商家再通知客户购买成功，将商品寄送客户。

2. SET 安全协议

在开放的因特网上处理电子商务，如何保证买卖双方传输数据的安全成为电子商务能否普及的最重要的问题。为了克服 SSL 安全协议的缺点，Visa 和 Master-Card 两大信用卡组织，联合开发了 SET 电子商务交易安全协议。这是一个为了在因特网上进行在线交易而设立的一个开放的、以电子货币为基础的电子付款系统规范。SET 在保留对客户信用卡认证的前提下，又增加了对商家身份的认证，这对于需要支付货币的交易来讲是至关重要的。由于设计合理，SET 协议得到了 IBM、HP、Microsoft、Netscape、VeriFone、GTE、VeriSign 等许多大公司的支持，已成为事实上的工业标准。目前，它已获得 IETF 标准的认可。安全电子交易是基于因特网的卡基支付，是授权业务信息传输的安全标准，它采用 RSA 公开密钥体系对通信双方进行认证，利用 DES、RC4 或任何标准对称加密方法进行信息的加密传输，并用 Hash 算法来鉴别消息真伪，有无涂改。在 SET 体系中有一个关键的认证机构（CA），CA 根据 X.509 标准发布和管理证书。

实验 11　域名服务

一、实验目的

掌握电子商务的域名设置。

二、实验原理

DNS 是域名系统（Domain Name System），是一种组织域层次结构的计算机和网络服务命名系统。它在本地负责控制整个分布式数据库的部分段，每一段中的数据通过客户/服务器模式在整个网络上均可存取，通过采用复制技术和缓存技术使得整个数据库可靠的同时，又拥有良好的性能。当用户在应用程序中输入 DNS 名称时，DNS 服务可以将此名称解析为与此名称相关的 IP 地址信息。

三、实验内容

南京奥派科技是一家提供域名和主机服务的公司，近期该公司在网上发布了一些关于域名和主机的信息。李明看到此信息之后，通过比较，购买了他们的域名和主机，事后并对购买的域名和主机进行管理。

四、实验步骤

1. 发布域名和主机信息

服务商（南京奥派科技）绑定银行账号，维护域名类别，发布域名信息、主机信息以及促销信息。另外，还要发布新闻、客户案例和联系方式。

（1）选择“网络营销实践”模块，选择“域名服务”选项，单击“服务商平台”后面的“进入”按钮，进入服务商平台。

(2) 单击"支付管理"标签,进入银行账户绑定界面,输入正确的服务商银行账户(这里的账号是在电子支付实践中所申请的企业账号),单击"提交"按钮,则服务商绑定银行账号成功,如图 7.1 所示。



图 7.1 银行账户绑定

(3) 服务商发布域名信息。首先服务商要添加域名类别,在"产品中心"选项卡中,单击左框中的"域名类别维护",在右框架中显示域名类型管理界面,单击"添加"按钮,输入所要添加的域名类别和描述,单击"保存"按钮,则域名类别添加成功,如图 7.2 所示。



图 7.2 添加域名

(4) 在"产品中心"选项卡中,单击左框中的"域名发布",在右框架中显示域名类型管理界面,单击"添加"按钮,进行新的域名发布,域名信息设置成功之后,单击"发布"按钮,发布该域名,如图 7.3 所示。

(5) 服务商发布主机信息。在"产品中心"选项卡中,单击左框中的"主机发布",在右框架中显示主机管理界面,单击"添加"按钮,进行主机发布设置,主机信息设置成功之后,单击"发布"按钮,发布该主机,如图 7.4 所示。

(6) 服务商发布新闻、客户案例、设置联系方式。在"新闻中心"选项卡中,进行新闻管理,单击左框架中的"新闻发布",在右框架中显示新闻管理界面,单击"添加"按钮,进行新闻发布,如图 7.5 所示。



图 7.3　域名发布



图 7.4　主机发布

(7) 在“新闻中心”选项卡中,单击左框架中的“客户案例”,在右框架中显示客户案例界面,单击“添加”按钮,发布新的客户案例,如图 7.6 所示。

(8) 在“新闻中心”选项卡中,单击左框架中的“客户联系方式”,在右框架中编辑客户联系方式,单击“保存”按钮即可。



图 7.5 新闻发布



图 7.6 案例发布

2. 域名和主机管理

注册会员李明，购买域名和主机，并对已购买的域名和主机进行管理。同时，也可以向服务商申请发票，并发送提问。另一方面，服务商进行会员管理、域名业务管理、域名解析、主机业务管理，并对发票进行审批，回答会员的提问。

(1) 注册会员。单击“域名服务平台”后面的“进入”按钮，进入域名服务平台界面。然后单击界面右上方的“注册”按钮，进入用户注册界面。

(2) 在用户注册界面，填写注册信息、个人资料、联系方法和附加信息等内容，填写完成之后，单击“注册”按钮，提交注册信息。

(3) 当新会员注册成功之后，系统会自动导航到登录界面，注意的是数字 ID 从右边

获得。输入昵称，单击右上角的“查询数字 ID”按钮即可。

(4) 购买域名。单击左上角的“进入账户”，进入“我的控制面板”，单击“产品购买”下拉列表中的“域名购买”。要先对所要购买的域名进行查询，在域名查询结果中，只有未被别人注册过的域名，才能注册，才能购买。

输入想要注册的域名，选择后缀(顶级域名)，单击“检测”按钮，检测该域名是否已被别人注册。如果该域名还没有被注册，单击“购买”按钮，进行域名购买，否则进行重新查询。

(5) 接下来，要进行域名注册，域名注册信息分为注册信息、注册人信息和附加信息部分。信息填写完毕，确认无误之后，单击“下一步”按钮，如图 7.7 所示。

域名注册(III 信息填写)

注册信息	
注册域名：	liming .com * 检测 该域名可以注册
域名密码：	●●●●●●
确认密码：	●●●●●●
注册人信息	
用户类型：	⊙ 公司 ○ 个人
公司/所有人(中文)：	南京舜天科技
公司/所有人(英文)：	nanjingshuntiankeji
注册联系人(中文)：	李明
注册联系人(英文)：	liming
省份(中文)：	江苏省 南京市
省份(英文)：	jiangsu
城市(英文)：	nanjing
邮政编码：	210000
地址(中文)：	福建路2号
地址(英文)：	fujianlu2hao
电子邮件：	liming@126.com 您常用的电子邮箱
电话号码：	15912345671
传真号码：	025-83491231
附加信息	
选择域名解析服务器：	⊙ 使用默认DNS服务器 ○ 您填写的DNS必须是国内注册过的DNS
DNS1：	231.231.2.1
DNS2：	231.231.2.0
	☑ 我已阅读、理解并接受注册协议

特别提醒您：

为了使您更快捷地注册域名，此处只需填写注册人信息，管理联系人请您在注册成功后登陆会员服务系统更改即可。

下一步　取　消

图 7.7　填写域名注册信息

(6) 域名注册完成之后，要进行域名的充值。选择所要充值的域名，单击“域名续费”图标，如图 7.8 所示。

(7) 在弹出的界面中选择付费年限、费用，单击“支付”按钮，进行支付。



图 7.8 域名续费

(8) 选择“中国工商银行”，单击“支付”按钮。再确认支付信息，单击“在线支付”按钮。

(9) 在“支付”界面，输入卡号、支付密码和附加码，单击“确定”按钮，如图 7.9 所示。



图 7.9 确认支付信息

(10) 购买主机。进入“我的控制面板”，单击“产品购买”下拉列表中的“主机购买”。在注册购买界面，单击主机信息下方的“购买”按钮。

(11) 接下来，要选择主机的配置资料(操作系统选择 UNIX，机房选择电信)，单击“购买”按钮，完成主机购买。注意，主机的默认密码是 88888888。

(12) 新购买的主机。要进行主机续费，单击“主机续费”图标。在弹出的界面中，选择年限及金额，单击“确认”按钮。

3. 思考题

怎么设置域名?

实验 12　网络广告

一、实验目的

利用软件来学习掌握网络广告,邮件推广和网络调研实践活动。

二、实验原理

网络广告,主要是指利用信息通信网络作为广告媒体,采用电子多媒体技术进行设计制作,并通过网络进行传播的广告形式。它是新世纪中经济社会生活的向导,并以其新的内涵成为一个新的焦点。

随着互联网的普遍应用,网络广告已经成为中国广告业一个闪亮明星,广告媒体已经成为今天的主流媒体和强势媒体。不过,这也要求我们对网络广告的发展有更清晰的认识,能根据广告业自身的发展,加大对网络广告的设计模式开发和创意研究。网络广告设计的创意需要传统创意人的灵感,也需要技术支持,因为创意的优势不仅仅是视觉、听觉等元素,还有广告形式上通过整合而制造的新互动。

三、实验内容

南京奥派科技是一家网络广告的提供商。李明是南京舜天科技的一名职员,主要负责公司的业务推广,现想在奥派科技的网络广告平台上申请网络广告。

四、实验步骤

1. 网络广告的发布商设置初始数据

网络广告的服务商(南京奥派科技)绑定银行账户,然后进行网络广告报价的设置以及发布新闻。另外,用户李明申请网络广告账号,服务商(南京奥派科技)对会员进行管理。

(1) 进入服务商平台。选择“网络营销实践”模块,选择“网络广告”选项,单击“服务商平台”后面的“进入”按钮,进入网络广告服务商平台。

(2) 服务商绑定银行账号。单击“支付管理”标签,进入“银行账户管理”界面,单击“新增账户”按钮。

(3) 在弹出的银行账号管理界面中,输入已申请的南京奥派科技的网上银行账号,单击“提交”按钮,则服务商银行账号绑定成功,如图 7.10 所示。



图 7.10　银行账号绑定

(4) 服务商广告报价管理。进入服务商平台,单击“报价管理”标签,进入报价管理界面,对于不同频道的不同广告位报价,只需输入新的报价,单击“修改”按钮,即可成功修改广告位报价。

(5) 用户申请网络广告账号。单击“网络广告平台”后面的“进入”按钮,进入网络广告平台界面。

(6) 单击左下角的“网络广告——让你的企业一夜成名”图标,进入用户界面。单击左上角的“注册”按钮,进入注册界面。

(7) 在用户注册界面中填写详细注册信息(用户名、登录密码、性别等),单击“确定”按钮,则会员注册成功。

(8) 服务商对会员进行管理。单击“服务商平台”后面的“进入”按钮,进入服务商平台,单击“会员管理”下拉列表中的“会员资料管理”,进入会员资料管理界面。单击操作下方的“详细”按钮可查看会员详细信息,单击“编辑”按钮可管理会员资料信息。

(9) 单击“会员管理”下拉列表中的“会员控制”,进入会员控制界面,单击操作下方的“控制”按钮,在弹出的会员信息控制界面中,选择会员状态(正常),单击“修改”按钮即可。

(10) 单击“会员管理”下拉列表中的“密码重置服务”,进入会员密码重置界面,单击操作下方的“密码重置”按钮。在弹出的密码重置界面中,填写重置原因,输入新密码和校对密码,单击“重置”按钮即可。

2. 用户申请网络广告并购买

作为会员的李明先要进行账户充值,并选择广告类型和发布时间,申请广告位。另一方面,服务商要审核该会员的广告申请。

(1) 用户修改个人信息。单击“李明”后面的“进入”按钮,进入用户界面。

(2) 单击左上角(李明)的“资料”按钮,进入注册信息维护界面。在注册信息维护之后,单击“修改”按钮即可。

(3) 用户进行账户充值。单击左上角(李明)的“在线充值”按钮,进入在线充值界面。选择中国工商银行,输入充值金额(1000),单击“去银行充值”按钮。

(4) 进行在线确认,单击“在线支付”按钮。

(5) 输入卡号、支付密码和验证码,单击“确认”按钮,则支付成功。

(6) 会员申请广告并管理广告。单击“广告申请”下的 Go 按钮,进入广告申请界面。填写广告申请详细信息,单击“确定”按钮,如图 7.11 所示。

(7) 如需撤销申请中的广告,单击“广告管理”下的“操作”下方的“详细”按钮,如图 7.12 所示。在弹出的界面中,单击“撤销申请”按钮,如图 7.12 所示。

(8) 如需修改申请中广告的信息,单击“操作”下方的“编辑”按钮(图 7.12),在弹出的界面中,填写修改的资料,单击“确定”按钮。

(9) 服务商广告业务管理。服务商对用户广告进行编辑,进入服务商平台,单击“业务中心”下拉列表中的“广告编辑”,单击操作下方的“编辑”按钮。在弹出的界面中编辑申请广告信息,单击“确定”按钮。

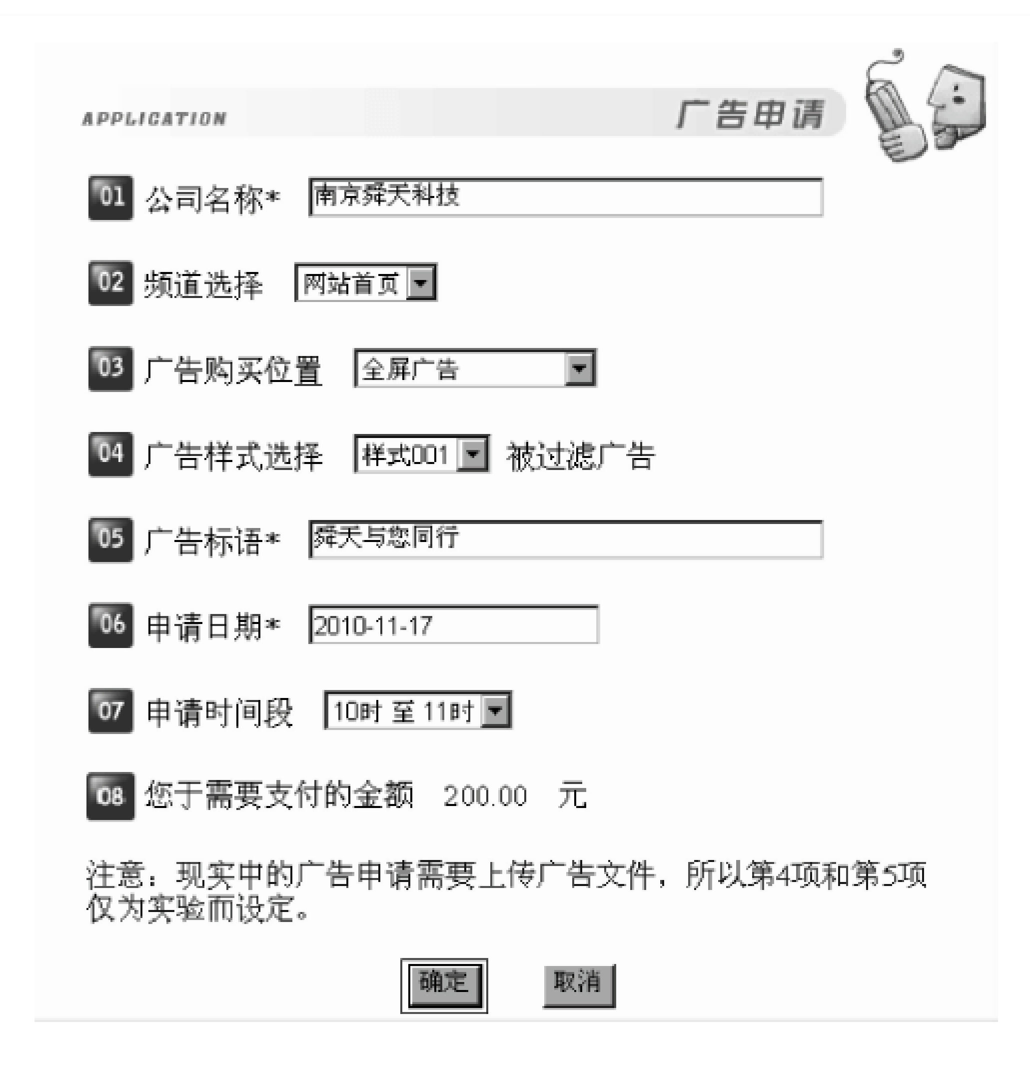


图 7.11　广告申请

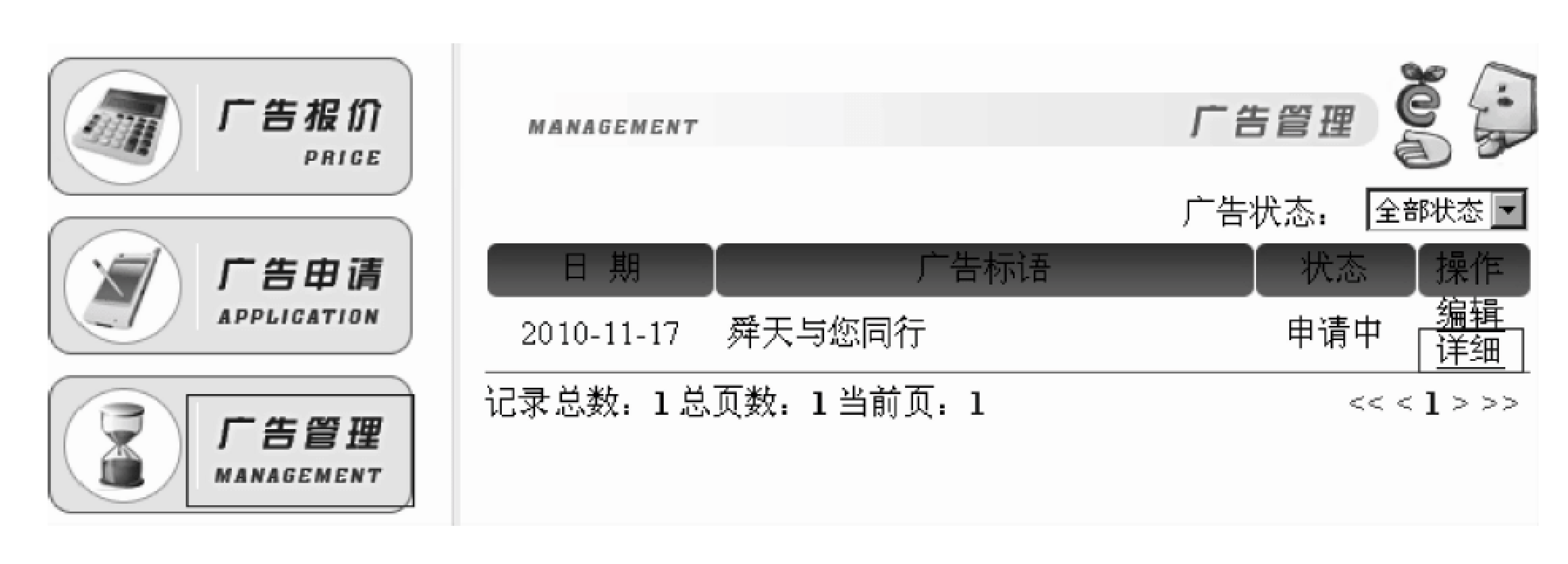


图 7.12　撤销广告申请

（10）服务商撤销用户广告。进入服务商平台，单击“业务中心”下拉列表中的“广告撤销”，单击操作下方的“撤销”按钮。

（11）服务商审核用户广告。进入服务商平台，单击“业务中心”下拉列表中的“广告安排”，单击操作下方的“审核”按钮。进入广告安排界面，单击“审核”按钮。

3. 申请效果管理和其他功能

服务商发布新闻，以及促销价的设置；另一方面，用户查看已发布的广告效果，并对服务商提问留言，服务商对其回复。

（1）服务商广告管理。服务商发布新闻，进入服务商平台，单击“广告管理”下拉列表中的“新闻管理”，进入新闻管理界面，单击“发布新闻”按钮。输入新闻主题和内容，单击“发布新闻”按钮，则新闻发布成功。

如需查看新闻内容，单击操作下方的“查看”按钮；如需编辑新闻内容，单击操作下方的“编辑”按钮；如需删除新闻内容，单击操作下方的“删除”按钮，如图 7.13 所示。



图 7.13 广告管理

(2) 服务商查看广告位单击效果。单击“广告管理”下拉列表中的“广告位单击效果”，进入广告位单击效果界面，选择所要查看频道的广告位，即可查看到广告位单击效果。

(3) 服务商设置广告位促销信息。单击“广告管理”下拉列表中的“广告位促销价设置”，进入广告位促销价设置界面，选择促销频道、促销广告位置和促销价格，单击“确定”按钮。

(4) 会员提问。单击李明后面的“进入”按钮，进入会员平台，单击“网络留言”下面的Go按钮，进入网络留言界面。单击“我要留言”按钮，进入留言界面。选择留言类型，填写留言标题和内容，单击“保存”按钮。

(5) 服务商回复留言。进入服务商平台，单击“用户留言”下拉列表中的“用户留言管理”，进入留言管理界面，单击操作下面的“回复”按钮。进入留言信息维护界面，查看用户留言内容，输入回复内容，单击“回复”按钮。

服务商如需删除留言，首先应选择所要删除的留言，再单击“删除”按钮即可。

(6) 服务商发送系统信息。进入服务商平台，单击“用户留言”下拉列表中的“消息群发”，输入群发消息标题和内容，选择接收会员，单击“发送”按钮。

(7) 会员查看留言。单击李明后面的“进入”按钮，进入会员平台，单击“网络留言”下面的Go按钮，进入网络留言界面，单击“系统消息”按钮，查看系统消息；单击回复留言后面的“查看”按钮，查看已恢复留言。

(8) 查看广告效果。单击“网络广告平台”后面的“进入”按钮，查看网络广告的效果。

4. 思考题

怎么取得良好的网络广告？

第8章

电子商务物流篇

8.1 引言

当今世界网络、通信和信息技术飞速发展，Internet 在全球迅速普及，使得商务空间发展到全球的规模，促进企业组织改革自己的思维观念、组织结构、战略方针和运行方式来适应全球性的发展变化。电子商务就是适应以全球为市场而出现和发展起来的一种新的商贸模式，通过网络技术快速而有效地进行各种商务行为，即在商务运作的整个过程中实现交易无纸化、直接化。电子商务可以使商家与供应商，在全球市场上销售产品；也可以让用户足不出户在全球范围内选择最佳商品，享受全过程的电子服务。

电子商务作为网络时代的一种全新的交易模式，相对于传统商务是一场革命。电子商务的优势之一就是能大大简化业务流程，降低企业运作成本，而电子商务企业成本优势的建立和保持必须以可靠和高效的物流运作作为保证。所以，加大力度防护物流信息的安全，大力发展现代化物流，电子商务才能得到更好的发展。

8.2 电子商务物流

8.2.1 电子商务与现代物流的概念

电子商务(Electronic Commerce，EC)，通常是指在全球各地广泛的商业贸易活动中，基于浏览器/服务器应用方式，买卖双方不谋面地进行各种商贸活动，实现消费者的网上购物、商户之间的网上交易和在线电子支付以及各种商务活动、交易活动、金融活动和相关的综合服务活动的一种新型的商业运营模式。

现代物流是以追求企业效益为目标，以现代化的手段与设备，以先进的管理与运作，

实现商品与服务的实体从供给者向需求者转移的经济活动过程。它包括分配计划、运输、仓储、市场研究、为用户服务五个方面的综合性服务。

8.2.2 电子商务与现代物流的关系

现代物流的发展与电子商务是密不可分的,可以从以下两个方面理解:

(1) 电子商务的应用改变了传统市场的结构,改变了传统的物流观念,改变了物流的运作方式,改变了物流企业的经营。从而使生产企业和消费者可以直接互联,让电子商务环境下供应链变得更为科学和合理。

(2) 物流是商流、资金流、信息流、物流这四流中最为特殊的一种。缺少了现代化的物流过程,电子商务就不再完整。物流还是实施电子商务的关键和支点,无论是在传统的贸易方式下,还是在电子商务下,生产都是商品流通之本,而生产的顺利进行需要各类物流活动支持,整个生产过程实际上就是系列化的物流活动。缺少了现代化的物流,生产将难以进行,无论电子商务是多么便捷的贸易方式,仍将是无米之炊。

8.2.3 电子商务下的物流模式

1. 自建物流

自建物流系统的核心是建立集物流、商流、信息流于一体的现代化新型物流配送中心,而电子商务企业在自建物流配送中心时,应广泛地利用条码技术、数据库技术、电子订货系统、电子数据交换、快速反应(QR)以及有效的客户反应(ECR)等信息技术和先进的自动化设施,以使物流中心能够满足电子商务对物流配送提出各种要求。

2. 第三方物流

在电子商务环境下发展第三方物流往往会为企业带来较为满意的结果,而第三方物流所带来的好处主要体现在减少成本、提高服务水平、增加灵活性、提高进入更大市场的可能性、增强市场反应能力、有利于业务流程的优化以及增加知识存量等方面。对于开展电子商务的企业而言,采用第三方物流模式解决物流问题具有明显的战略优势,主要表现为:①企业集中精力于核心业务;②灵活运用新技术,实现以信息换库存,提供灵活多样的顾客服务,为顾客创造更多的价值;③减少固定资产投资,加速资本周转。

3. 第四方物流

第四方物流的概念最早由安达信咨询公司提出的。按照 John Gattorna 的定义,第四方物流供应商是一个供应链的集成商,它对公司内部和具有互补性服务供应商所拥有的不同资源、能力和技术进行整合和管理,提供一整套供应链解决方案。从第四方物流的内涵来看,第四方物流不仅控制和管理特定的物流服务,而且对整个物流过程提出策划方案,并通过电子商务将这个过程集成起来,所以,第四方物流成功的关键在于为顾客提供最佳的增值服务,即迅速、高效、低成本和人性化服务。

4. 精益物流和敏捷物流

精益思想的核心是“通过彻底排除浪费来降低成本”。它的具体要求就是在适当的

时间、适当的地点提供适量的零部件，这种与供应链管理的思想密切融合起来的物流配送就是精益物流的雏形。敏捷制造和动态联盟的概念最初在美国里海大学向美国国会提交的一份研究报告中提出，很快便受到了国会和工业办的普遍重视，目前几乎所有的美国大公司都接受敏捷制造的思想，同时世界上其他的发达国家也纷纷进行敏捷思想的研究和应用。

5. 发展物流联盟

《物流术语》中这样定义物流联盟：为了达到比单独从事物流活动所取得的更好效果，企业间形成的相互信任、共担风险、共享利益的物流伙伴关系。企业间不完全采取导致自身利益最大化的行为，也不完全采取导致共同利益最大化的行为，只是在物流方面通过契约形成优势互长、要素双向或多向流动的中间组织。狭义的物流联盟存在于非物流企业之间，广义的物流联盟包括第三方物流。发展现代物流，就是要发展以第三方物流为基础的，构建物流企业与非物流企业乃至物流企业与物流企业间的巩固的物流联盟，这两种物流联盟的基础不同，物流企业与非物流企业之间的基础是服务；物流企业与物流企业之间的基础是制度服务规则。

8.2.4　电子商务环境下物流的发展趋势

电子商务环境下物流的发展趋势如下：

(1) 物流服务功能不断扩展基于电子商务的现代物流，除了满足传统物流的基本功能外，主要是提供的广阔的增值服务(ValueAdded Logistics Services)功能。增值性的物流服务包括：①增加便利性的服务，一切能够简化手续、简化操作的物流服务都属于此类，如自动订货、传递信息和转账等；②加快反应速度(Quick Response)的服务，在需求方对速度的要求越来越高的情况下，快速反应已经成为物流发展的动力之一；③延伸服务，向上可以延伸到市场调查与预测、采购及订单处理，向下可以延伸到配送、物流咨询、物流方案的选择与规划等；④降低成本的服务，电子商务发展的前期，物流成本将会高居不下，有些企业可能会因为根本承受不了这种高成本退出电子商务领域，或者是选择性地将电子商务的物流服务外包出去，这是很自然的事情，因此发展电子商务，一开始就应该寻找能够降低物流成本的物流方案。

(2) 物流的全球化趋势电子商务发展打破了时空限制，经济全球化特点日益明显，在现代企业产品跨国界流通的形势下，物流企业的服务范围也相应地从区域向全球扩展。全球化战略的趋势，使物流企业和生产企业更紧密地联系在一起，生产企业致力于制造产品、降低成本、创造价值的同时，物流企业要集中精力提高物流服务需求，做好物流服务。例如，在配送中心，对进口商品的代理报关业务、储存、搬运和配送，必要的流通加工，从商品进口到送交消费者手中的实现一条龙服务。在电子商务环境下发展物流业是时代所趋，要正确认识电子商务对物流业的影响和促进作用，合理地选择电子商务成本的投入，从而增加我国物流行业的竞争力。

8.3 与电子商务安全有关的技术

8.3.1 密码技术

密码技术根据密钥性质的不同,可分为传统密码体制和公开钥密码体制两大类型。传统密码体制加密解密用同一个密钥,即 Ke=Kd;而公开钥密码体制使用一对密钥即一个私钥和一个公钥,其对应关系是唯一的,公钥对外公开,私钥个人秘密保存。一般用公钥来进行加密,用私钥来进行签名;同时私钥用来解密,公钥用来验证签名。算法的加密强度主要取决于选定的密钥长度。

8.3.2 访问控制

除了计算机网络硬件设备之外,网络操作系统是确保计算机网络安全的最基本软件。它是计算机网络资源的管理者,必须具备安全的控制策略和保护机制,防止非法入侵者攻破设防而非法获取资源。网络操作系统安全保密的核心是访问控制,即确保主体对客体的访问只能是授权的,未经授权的访问是不允许的,其操作是无效的。因此,授权策略和机制的安全性显得特别重要。保护可以从以下几个方面加以考虑:物理隔离、时间隔离、密码隔离。

8.3.3 防火墙技术

设立防火墙的目的是保护内部网络不受外部网络的攻击,以及防止内部网络用户向外泄密。目前,防火墙技术主要有分组过滤和代理服务两种类型。

(1) 分组过滤:是一种基于路由器的防火墙。它是在网间的路由器中按网络安全策略设置一张访问表或黑名单,即借助数据分组中的 IP 地址确定什么类型的信息允许通过防火墙,什么类型的信息不允许通过。防火墙的职责就是根据访问表(或黑名单)对进出路由器的分组进行检查和过滤,凡符合要求的放行,不符合的拒之门外。这种防火墙简单易行,但不能完全有效地防范非法攻击。目前,80%的防火墙都是采用这种技术。

(2) 代理服务:是一种基于代理服务的防火墙。它的安全性高,增加了身份认证与审计跟踪功能,但速度较慢。所谓审计跟踪是对网络系统资源的使用情况提供一个完备的记录,以便对网络进行完全监督和控制。通过不断收集与积累有关出入网络的完全事件记录,并有选择地对其中的某些记录进行审计跟踪,发现可能的非法行为并提供有力的证据,然后以秘密的方式向网上的防火墙发出有关信息,如黑名单等。

8.3.4 数字时间戳

交易文件中,时间是十分重要的信息。在书面合同中,文件签署的日期和签名一样均是十分重要的防止文件被伪造和篡改的关键性内容。在电子交易中,同样需对交易文件的日期和时间信息采取安全措施,而数字时间戳服务(Digital Time-stamp Service,

DTS)就能提供电子文件发表时间的安全保护。

数字时间戳服务(DTS)是网上安全服务项目,由专门的机构提供。时间戳(Time-stamp)是一个经加密后形成的凭证文档,它包括需加时间戳的文件的摘要(Digest)、DTS收到文件的日期和时间和DTS的数字签名。

中国电子商务认证系统建设中出现的问题,客观上引导CA向一个更加理性、更加实际的方向发展,并将促使中国的电子商务循序渐进地前进。随着时间的推移,电子商务将从根本上改变几千年来形成的传统商业模式,充分体现现代科学技术给人们生活所带来的便利。

8.3.5　数字证书

在交易支付过程中,参与各方必须利用认证中心签发的数字证书来证明各自的身份。所谓数字证书,就是用电子手段来证实一个用户的身份及用户对网络资源的访问权限。

数字证书是用来唯一确认安全电子商务交易双方身份的工具。由于它由证书管理中心做了数字签名,因此任何第三方都无法修改证书的内容。任何信用卡持有人只有申请到相应的数字证书,才能参加安全电子商务的网上交易。数字证书一般有四种类型:客户证书、商家证书、网关证书及CA系统证书。

8.4　电子商务网上支付存在的问题

8.4.1　网上支付的安全问题

造成网上支付发展的安全风险主要有三个方面:一是银行网站本身的安全性;二是交易信息在商家与银行之间传递的安全性;三是交易信息在消费者与银行之间传递的安全性。无论是何种风险,其根本原因都是由于登录密码或支付密码泄露造成的。

(1) 密码管理问题。大部分公司和个人受到网络攻击的主要原因是密码政策管理不善。大多数用户使用的密码都是字典中可查到的普通单词姓名或者其他简单的密码。有86%的用户在所有网站上使用的都是同一个密码或者有限的几个密码。许多攻击者还会直接使用软件强力破解一些安全性弱的密码。因此,建议用户使用复杂的密码,降低被病毒破译密码的可能性,提高计算机系统的安全性。需要注意的是:一是密码不要设置为姓名、普通单词、电话号码、生日等简单密码;二是结合大小字母、数字共组密码;三是密码位数应尽量大于9位。

(2) 网络病毒、木马问题。现今流行的很多木马病毒都是专门用于窃取网上银行密码而编制的。木马会监视IE浏览器正在访问的网页,如果发现用户正在登录个人银行,直接进行键盘记录输入的账号和密码,或者弹出伪造的登录对话框,诱骗用户输入登录密码和支付密码,然后通过邮件将窃取的信息发送出去。

(3) 钓鱼平台。“网络钓鱼”攻击者利用欺骗性的电子邮件和伪造的Web站点来进

行诈骗活动，如将自己伪装成知名银行、在线零售商和信用卡公司等可信的品牌。受骗者往往会泄露自己的财务数据，如信用卡号、账户号和口令等。

8.4.2 网上支付的信用问题

在网络支付中由于其虚拟性、超时空性等特点，使双方互不相见，也难以客观地判断对方的信用等级，致使网络支付双方对对方的信用产生怀疑，也因此阻碍了网络支付的发展。

8.4.3 网上支付的法律问题

目前制约网上支付发展的立法问题主要包括：谁来发行电子货币；如何进行网络银行的资格认定；怎样监管网络银行的业务等。目前中国在电子商务方面，有关的政策不够明朗化，相应的法律法规、标准还都没有建立，跨部门、跨地区的协调存在较大的问题。

1. 网上安全认证机构(CA)建设混乱

在网络上，为了完成交易，交易双方的身份都必须通过第三方得到确认，电子商务认证机构由此产生。电子认证机构的职责是核实使用者的身份，负责电子证书的发放管理，及时公布无效的证书。

2. 缺乏相应法律法规

目前，具体到为电子商务服务的网上支付业务，法律上基本还是一个空白。传统的支付结算规则在网上支付业务规范中有一定的作用，但局限性很大。另外，目前涉及网上支付的法律只有《电子签名法》(解决了类似传统结算业务中签章的问题)，规章有人民银行发布的《网上银行业务管理办法》、银监会的《电子银行业务管理办法》和人民银行的《电子支付指引》，除此没有其他规范。如果从近期讨论的为电子商务服务的网上支付问题来看，法律制度上几乎一片空白。法律法规的缺失，导致政府机构对目前从事网上支付业务的这些机构和他们的业务要不要监管，要不要有一定的规则去规范缺乏统一标准。正是因为法律法规建设的滞后导致了网上支付存在的一系列问题，包括安全问题、金融监管问题、消费者权益保护问题等。

8.5 完善我国电子商务网上支付的对策

8.5.1 安全技术策略

为了确保通信的安全性，必须采取必要的措施加以防范。在通信连接方面，可以使用防火墙、代理服务器、虚拟专用网络(VPN)等技术；在鉴别和认证方面，可以采取加密和认证技术。做好自身计算机的日常安全维护，注意以下几点：一是经常给计算机系统升级；二是安装杀毒软件、防火墙，经常升级和杀毒；三是在平时上网时尽量不上一些小型网站，选大型网站，知名度比较高的网站，避免网站挂有病毒、木马造成中毒；四是尽量

不要在公共计算机上使用自己的有关资金的账户和密码，五是有条件的情况下，在初装计算机操作系统后，给自己的计算机做上备份，在使用资金账户前做一次系统恢复。

8.5.2 加快立法进程，完善法律保障

我国电子商务立法还不够，我国没有制定专门的电子支付法，仅有一些行业规范效力等级不高，传统支付法律体系中关于现金与票据清算的规则并不能完全适应网上支付的出现与发展；在电子资金划拨方面，《中华人民共和国票据法》确立的是以纸质票据为基础的结算支付制度，没有针对电子资金划拨进行立法，这严重阻碍了电子商务的发展。2005年6月公布的《电子支付指引》被看做是继《电子签名法》之后，政府为推动电子商务发展而实施的又一重大措施。我们应当趁着势头加快《电子支付法》等立法进程，完善有关配套法规制度。

1. 提高危机意识，应对网络犯罪

网上支付出现后，为洗钱等新型犯罪活动提供了新的机会和更大的空间。犯罪行为人利用各种先进的计算机技术来盗取信用卡信息、私人资料及金融财政内部资料，然后进行网上金融诈骗等犯罪。我国现行新《刑法》虽然对计算机网络犯罪等做出了相关规定，但从广度和深度来说都还不够，而随着国际网络发展以及电子商务的扩展，对出现的新型犯罪应给予足够的重视，通过相关立法来制裁此类犯罪，真正做到有法可依。

2. 加强社会信用机制建设

法律为保障网上支付必须推动社会信用制度的建立。发达的商业社会对社会包括个人的信用有着很高的要求，并通过一系列公开透明的制度来维护和保障信用制度体系。我国目前在对信用概念内涵的理解、信用信息公开的方式和程度、信用服务企业的市场发展程度，以及对失信者的惩戒制度方面都还十分落后，甚至存在空白。应当承认我国还属于非诚信国家，信用制度还很不健全。我们应当着手网上支付信用机制的建设，建立个人社会信用体系，网络交易采用实名制，普及CA认证，及时收集和反馈用户信息并做出相应解决方案，促进用户建立网络信用。

3. 加强对网络银行、认证机构的监管

加强电子商务行业的监管，规范市场主体行为。首先，要加强对网络银行的监管。网上银行不同于传统银行，应该制定新的准入条件，加强对客户开户的监管，落实责任审查客户资料等信息，明确网上银行业务终止条件、清算办法等，制定电子货币退出机制，规范电子货币市场。其次，要加强对认证机构的监管。政府主管机关必须对认证机构进行监管，认证机构应制定严格的认证操作规则、定期审查制度以及信息控制制度，保证程序上的合法性，对于认证机构的违反行为要给予惩罚。最后，第三方支付机构应受银监会监督。第三方无权动用客户资金，必须确保资金安全和支付的效率。而支付中介的仲裁功能还未受到任何监管，其公正性应得到保证，因为其决策将直接作用于电子商务本身，影响交易的最终结果。

4. 完善的管理策略

由于电子商务交易系统是一个人机高度综合的系统，除了网络的安全之外，管理人员的管理也是非常重要的，而且是起决定性作用的因素。因此，对整个系统的管理权限的分配和监督、管理人员的培训和考核、道德和业务水平的培养都必须制定出一套完整的规章制度，以利于培养管理人员敬业爱岗的精神。

实验 13 电子商务物流仓储实践

一、实验目的

利用该软件来学习掌握电子商务物流仓储的基本运作。

二、实验原理

仓储是产品生产、流通过程中因订单前置或市场预测前置而使产品、物品暂时存放。它是集中反映工厂物资活动状况的综合场所，是连接生产、供应、销售的中转站，对促进生产提高效率起着重要的辅助作用。同时，围绕着仓储实体活动，清晰准确的报表、单据账目、会计部门核算的准确信息也同时进行着，因此仓储是物流、信息流、单证流的合一。

根据系统功能要求进行数据库中表格的建立。通过对用户的需求分析，需要记录物品的基本信息、仓库的基本信息和仓库的操作信息。

(1) 物品的基本信息表包括物品的编号、名称、生产厂商、种类、规格、等级和物品所属的客户，其中物品的编号为主键。因此，要建立一个物品列表，用以储存物品的信息。同时需要为物品基本信息中生产厂商、物品种类和客户建立单独的表。在物品的生产厂商表中包含生产厂商的名称和代号，生产厂商代号为主键；在物品种类表中包含物品种类的名称和代号，物品种类代号为主键；在客户表中包含客户的名称、联系人和联系电话，客户代号为主键。这样的设计完全满足 BCNF 范式，表格之间的条理比较清晰。各个表之间的主键关系如下：生产厂商表的主键与物品列表中的生产厂商代号相关联；物品种类表的主键与物品列表中的生产厂商代号相关联；客户表的主键与物品列表中的客户代号相关联。

(2) 仓库的基本信息应包括用于记录职工基本信息的仓库人员管理表和用于记录仓库库位信息的仓库信息表。仓库人员管理表中包括职工的代号、姓名、职位、联系电话、身份证号码和住址，职工代号为主键。仓库信息表中包括存放地点(相当于库位的标号)、仓库号、区域、货架号、层、行、列、是否为空几个属性，其中存放地点为主键。

(3) 仓库的操作信息应包括用于储存入库、出库及库内移动操作记录的入库表、出库表及库内移动表；用于储存当前仓库中物品记录的库存表；用于记录员工增删情况的人事变动表。入库表中应该记录物品的编码、入库的时间、经手人和存放地点，其中以物品编码和入库时间联合作为主键；出库表中应该记录物品的编码、出库时间和经手人，其中以物品编码和出库时间联合作为主键；库内移动表中应该记录物品的编码、移动时间、经手人、原存放地点和新存放地点，其中以物品编码和移动时间联合作为主键；库存表中应

该包括物品的编码、入库时间、存放地点和经手人，其中以物品的编码作为主键。人事变动表中应该包括操作号、人事变动的内容、变动的时间、变动人员的代号和变动人员的姓名，其中操作号为主键。另外，系统中还需要有用户的登录信息表用于记录用户的登录信息。登录信息表中应该有登录的用户名和密码，其中登录名为主键。为安全起见，在设计登录界面密码及储存于数据库时，系统采用 MD5 加密算法。

三、实验内容

南京奥派仓储公司是一家仓储公司，该公司想建立自己的仓储系统平台，在该平台中对自己的仓库和业务进行管理。

四、实践步骤

1. 基础数据设置

注册仓储公司(南京奥派仓储公司)的基本信息，并设置该公司的基础数据信息，包括：产品信息、出入库方式、库区的设置以及费用的设置，并对客户进行管理。

选择“电子商务物流实践”中的“仓储实践”图标，单击仓储管理员后面的“进入”按钮，进入仓储实践平台。首次登录要先设置仓储公司的基本信息，这也是进入仓储管理系统的第一步。填写完毕后单击“保存”按钮，提交仓储公司设置，如图 8.1 所示。

仓储公司名称:	南京奥派仓储公司	*
法人代表:	李明	*
注册资金:	1000万元	*
所在城市:	江苏省 南京市	*
公司地址:	福建路1号	*
联系电话:	025-83405213	*
E-Mail:	liming@126.com	
网址:	http://www.allpass.com.cn	
开户银行:	南京银行	*
银行帐号:	1111 2222 3333 4444	*(例：1111 2222 3333 4444)
公司简介:	南京奥派仓储公司为企业提供商品储存、整合、配送、生产支付等服务。	

图 8.1　填写仓储基本信息

如需修改仓储公司信息，单击左框架“系统管理”下拉列表中的“公司信息”，进入仓储公司基本信息维护界面，在右框架中显示已经设置的公司信息，修改相关信息后，单击“保存”按钮，提交修改设置。

2. 设置实践产品

(1) 单击左框架“基础设置”下拉列表中的“实验产品”，进入实践产品信息设置界面。首先，要进行产品行业管理。输入行业名称、行业编码前缀、行业介绍后单击“添加”按钮，提交行业信息设置。

添加完行业信息之后，还要添加该行业的下属产品。单击行业信息记录中"下属产品"下方的按钮，进入下属产品管理界面（如需查看行业说明，单击"行业说明"下方的按钮；如需修改行业信息，单击"修改"下方的按钮），如图 8.2 所示。



图 8.2 下属产品管理界面

在弹出的界面中，单击下方的"添加"按钮，添加下属产品，如图 8.3 所示。输入下属产品相关信息，单击"保存"按钮，提交产品信息。

产品信息添加

所属行业:	日用化工	产品编码:	RIG10001
产品海关名称:	1000	产品名称:	安利洗发露 *
产品海关编码:	100	产品规格:	V1.0
保质期(天):	180	保质期管理:	☑ 选择
产品单位(数量):	瓶 *	产品单位(重量):	克 *
产品单位(体积):	毫升 *	货币单位:	人民币 *
毛重:	100 *	净重:	80 *
体积:	10 *	采购价:	80 *
销售价:	150		

图 8.3 添加下属产品信息

（2）添加出库方式。单击左框架"基础设置"下拉列表中的"出库方式"，进入出库设置界面。出库方式是货物在出库时可选择的几种方式，如"自提"、"送货"、"代运"等，也可根据不同仓储公司的具体情况设置对应的其他出库方式。填写完毕后单击"添加"按钮即可。

（3）仓库设置。单击左框架"基础设置"下拉列表中的"仓库设置"，进入仓库设置界面。输入仓库的基本信息如仓库编号、仓库名称、地址、负责人以及选择前面设置的仓库类型和出库方式等内容，填写完毕后单击"添加"按钮即可（这里可以多设置几个仓库信息），如图 8.4 所示。

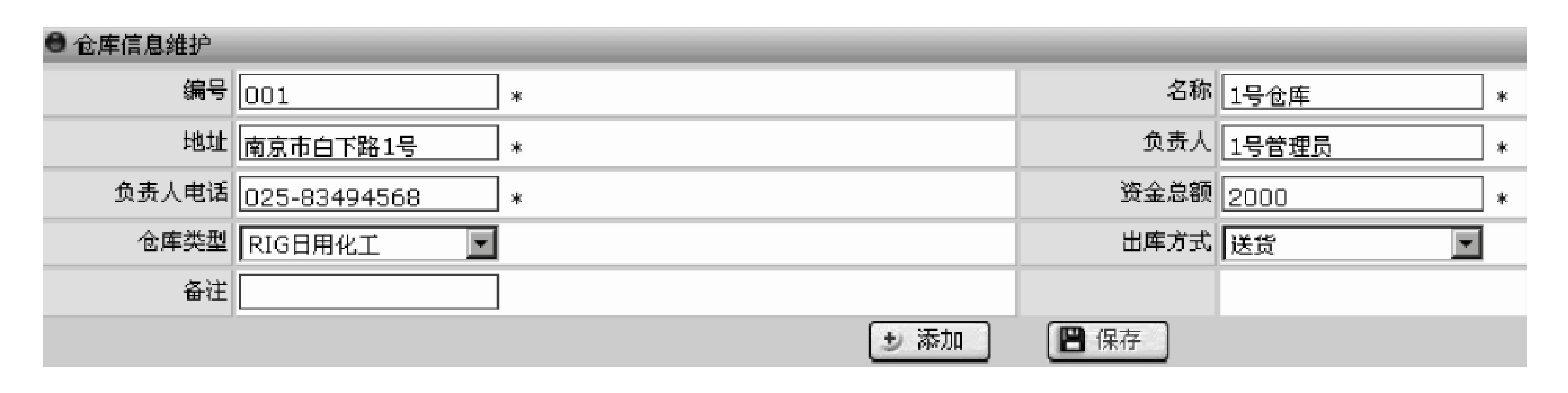


图 8.4 添加仓储设置

（4）库区设置。库区是从属仓库的，也是货物的存放位置。单击左框架"基础设置"下拉列表中的"库区设置"，进入库区设置界面。设置库区的编号、名称、容积、出租价格等。填写完毕后单击"添加"按钮即可（这里可以多设置几个库区信息），如图 8.5 所示。



图 8.5　库区设置

(5) 劳务价格设置。劳务价格即是在仓库管理中产生的与人员活动相关的费用，如包装费、上货架费等，在此系统中计价类别一般以重量计算，当货物的体积(立方米)/重量(千克)＞50 时以体积计。单击左框架“基础设置”下拉列表中的“劳务价格”，进入劳务费率信息维护界面，填写相关信息之后，单击“添加”按钮即可，如图 8.6 所示。

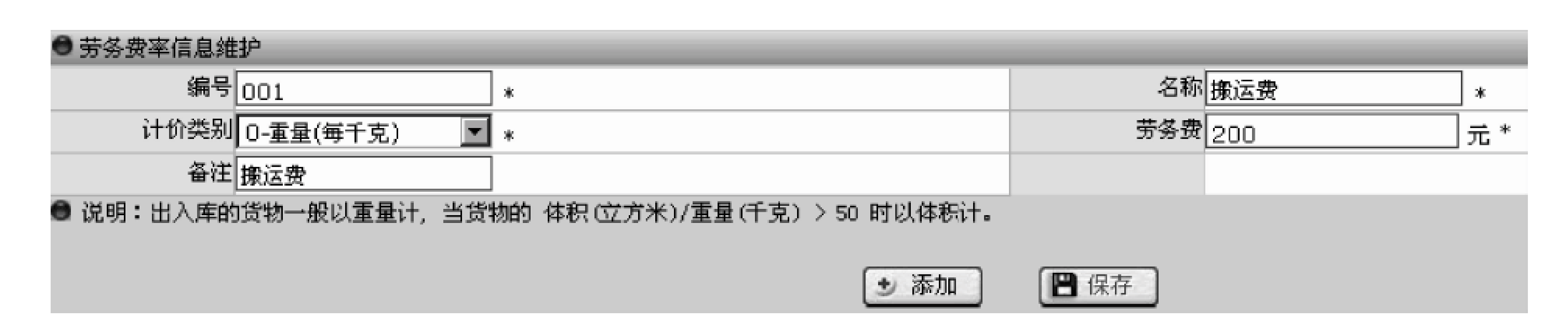


图 8.6　劳务价格设置

(6) 入库类型设置。入库类型就是货物在入库时采取的什么方式，如预定入库、调整入库、盘点入库、包装入库、报废入库等内容。单击左框架“基础设置”下拉列表中的“入库类型”，进入入库类型维护界面，填写相关信息之后，单击“添加”按钮即可，如图 8.7 所示。



图 8.7　入库类型设置

(7) 出库类型设置。出库类型是与入库类型相对应的，也是基于类似的设置。单击左框架“基础设置”下拉列表中的“出库类型”，进入出库类型维护界面，填写相关信息之后，单击“添加”按钮即可，如图 8.8 所示。

3. 客户管理

(1) 发布库区。单击左框架“客户管理”下拉列表中的“发布库区”，进入库区发布管理界面。这里的库区即是在基础设置中所添加的所有库区，其中蓝色的表示已经发布出



图 8.8 出库类型设置

去的，灰色的表示还没有发布的库区，库区只有发布出去才能被客户使用。选择未发布的库区，单击“发布”按钮，发布库区；选择已经发布的库区，单击“收回”按钮，取消库区发布，如图 8.9 所示。



图 8.9 发布库区

（2）客户信息管理。单击左框架“客户管理”下拉列表中的“客户信息”，进入客户信息管理界面。填写相关信息之后，单击“添加”按钮即可，如图 8.10 所示。



图 8.10 客户信息管理

（3）申请单管理。申请单管理是对库区的申请方管理，单击左框架“客户管理”下拉列表中的“申请单管理”，在客户申请单维护界面中填写相关信息，单击“添加”按钮即可，如图 8.11 所示。

对于要处理的单据先选择“通过”或“拒绝”，然后单击“审批”按钮即可。注意，审批后的单据是可以修改的，即可以重新审批进行状态更新，但是“审核”后的单据是不能修



图 8.11　申请单管理

改的。审核通过的库区就可以给需方用来存储货物了(先进行审批后进行审核,不同的颜色对应相应的状态)。

4. 业务处理

(1) 产品入库处理。单击左框架“业务处理”下拉列表“出入库”中的“入库单”,进入入库单管理界面,单击下方的“添加”按钮即可。

(2) 进入入库单编辑界面,单击备注信息,然后在“备注信息”下拉列表框中选择入库类型,单击“保存”按钮,如图 8.12 所示。



图 8.12　入库管理

(3) 在弹出的界面中单击“确定”按钮,再单击下方的“添加”按钮,进入入库产品设置界面,如图 8.13 所示。



图 8.13　入库产品

(4) 设置产品入库信息,选择货物名称以及入库库区,单击“确定”按钮,提交入库产品信息的设置(注意当仓库类型不符或是仓库空间不够的话,在入库库区中将没有可选库区),如图 8.14 所示。

(5) 再次选择“出入库”中的“入库单”,单击“审核”按钮,对入库单进行申请处理,但是已经审核的单据是不能编辑的。



图 8.14　入库产品信息

（6）产品出库处理。产品出库处理操作相当于入库处理的操作，单击左框架“业务处理”下拉列表“出入库”中的“出库单”，进入出库单管理界面，单击下方的“添加”按钮即可。进入出库单编辑界面，单击备注信息，然后在“备注信息”下拉列表框中选择出库类型，单击“保存”按钮，如图 8.15 所示。

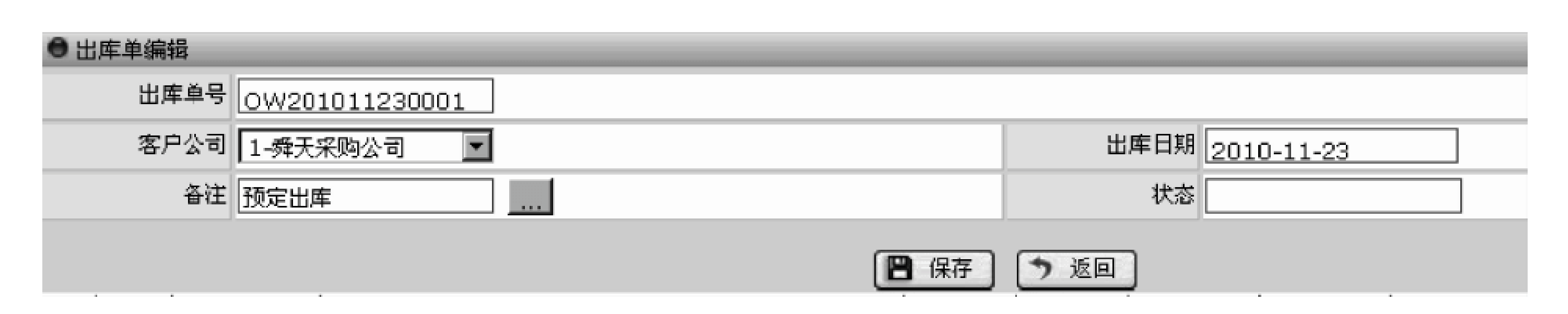


图 8.15　出库产品

（7）单击下方的“添加”按钮，进入出库产品设置界面，在弹出的界面中填写发货的数量（发货的数量不能大于库存数量），单击“确定”按钮；再进入“出库单”，单击“审核”按钮，对出库单进行处理。

5. 其他业务

（1）调拨单处理。调拨单是将库区中的货物调配的单据。如可将 a 库区中的部分货物调到 b 库区，首先 a 库区和 b 库区必须是同一类型的库区；其次 a 库区和 b 库区必须是同一家公司申请的。单击左框架“业务处理”下拉列表“其他业务”中的“调拨单”，进入调拨单列表界面，单击“添加”按钮，进入产品单据信息，如图 8.16 所示。

（2）进入产品单据信息后，单击记录信息后的“调拨”按钮，进入调拨设置界面，如图 8.17 所示。

（3）进入调拨设置界面后，选择调拨入库区，输入调拨数量和备注信息后，单击“保存”按钮，提交调拨设置，如图 8.18 所示。

（4）再次单击“调拨单”，进入“调拨单列表”界面，选择所要审核的调拨单，单击“审核”按钮即可，如图 8.19 所示。



图 8.16　调拨单处理

库存货物调拨

序号	库存量编号	货物编码	货物名称	数量单位	库存数量	存货库区	客户公司	调拨
1	XC201011230001	RIG10001	安利洗发露	瓶	10	1-1号仓库_1号库区	1-舜天采购公司	

图 8.17　库存调拨

产品调拨

调拨单号	MG201011230001	调拨日期	2010-11-23
库存编号	XC201011230001	客户公司	1-舜天采购公司
货物编号	RIG10001	货物名称	安利洗发露
库存位置	1-1号仓库_1号库区	拨入库区	2-1号仓库_2号库区
库存数量	10	调拨数量	2
数量单位	瓶	备注信息	调拨2

图 8.18　库存调拨设置

调拨单列表

*	序号	制单日期	调拨单编号	货物编码	货物名称	数量单位	调拨数量	
☑	1	2010-11-23	MG201011230001	RIG10001	安利洗发露	瓶	2	1-1号

图 8.19　调拨单审核

（5）盘点单处理。盘点单主要是盘点库存数量的，即看盘点后的数量比库存显示的数量是多了还是少了。选择左框架“业务处理”下拉列表“其他业务”中的“盘点单”，进入盘点单列表界面，单击“添加”按钮，进入产品单据信息。单击记录信息后的“盘点”按钮，进入盘点设置界面，如图 8.20 所示。

库存货物盘点

序号	库存量编号	货物编码	货物名称	数量单位	库存数量	存货库区	客户公司	盘点
1	XC201011230003	RIG10001	安利洗发露	瓶	2	2-1号仓库_2号库区	1-舜天采购公司	
2	XC201011230002	RIG10001	安利洗发露	瓶	10	1-1号仓库_1号库区	1-舜天采购公司	
3	XC201011230001	RIG10001	安利洗发露	瓶	8	1-1号仓库_1号库区	1-舜天采购公司	

图 8.20　盘点单处理

(6) 在盘点设置界面中，输入盘存数量和备注信息后，单击“保存”按钮，提交盘点设置，如图 8.21 所示。

产品盘点

盘点单号	TG201011230001	盘点日期	2010-11-23
库存编号	XC201011230003	客户公司	1-舜天采购公司
货物编号	RIG10001	货物名称	安利洗发露
库存位置	2-1号仓库_2号库区	数量单位	瓶
库存数量	2	盘存数量	3
备注信息	多出一个		

图 8.21 盘点设置

(7) 再次单击“盘点单”，进入盘点单列表界面。在盘点单列表中，选择盘点单，单击“审核”按钮，提交审核处理。

(8) 库存量整理。库存量是对库存的查询和整理操作。单击左框架“业务处理”下拉列表“其他业务”中的“库存量”，进入库存量整理界面，单击“整理”按钮可把已经发完货的单据自动删除掉。

6. 费用结算

费用单据显示的是出库、入库、出租的相关费用单据。单击左框架“业务处理”下拉列表“费用结算”中的“费用单据”，进入费用结算界面，对未缴费的单据可单击“催费”操作，即可向客户催收费用，如图 8.22 所示。

MENU
仓储系统平台
系统设置
基础设置
客户管理
业务处理
出入库
其他业务
费用结算
费用单据
收益查询
仓储分析
库龄分析

费用结算

序号	单据编号	制单日期	单据名称	客户公司	费用金额	单据状态	明细	操作
1	MB201011230001	2010-11-23	出租费用单	舜天采购公司	73200	未缴费	查看	催费
2	MB201011230002	2010-11-23	入库费用单	舜天采购公司	200000	未缴费	查看	催费
3	MB201011230003	2010-11-23	出库费用单	舜天采购公司	0	未缴费	查看	催费
4	MB201011230004	2010-11-23	入库费用单	舜天采购公司	200000	未缴费	查看	催费
5	MB201011230005	2010-11-23	出租费用单	舜天采购公司	36200	未缴费	查看	催费
合计					509400.00			

图 8.22 费用结算

7. 财务管理

仓储公司收益查询，包括出租收益和劳务收益两部分的查询；仓储公司进行仓储分析，包括安全库存、超储预警、低储预警、统计分析四部分的分析；另外，仓储公司还可以进行库龄分析，有两种类型，一是按年分析，另一个是按月分析。

(1) 出租收益查询。单击左框架“收益查询”下拉列表中的“出租收益”，在右框架中即可查看到出租收益，如图 8.23 所示。



图 8.23 出租收益

同样的，要查看入库劳务收益，就单击“劳务收益”下拉列表中的“入库劳务收益”；要查看出库劳务收益，就单击“劳务收益”下拉列表中的“出库劳务收益”，图 8.24 显示的是入库劳务收益。

入库收益

序号	单据编号	制单日期	单据名称	客户公司	费用金额
1	MB201011230002	2010-11-23	入库费用单	舜天采购公司	200000
2	MB201011230004	2010-11-23	入库费用单	舜天采购公司	200000
合计					400000

图 8.24　入库劳务收益

（2）仓储分析：仓储分析是对仓库的库存安全方面的统计分析(包括安全库存、超储预警、低储预警、统计分析)。

① 安全库存。安全库存是查询库区使用比例在 10%～60%的库区情况，单击左框架“仓储分析”下拉列表中的“安全库存”，即可查看安全库存信息，如图 8.25 所示。

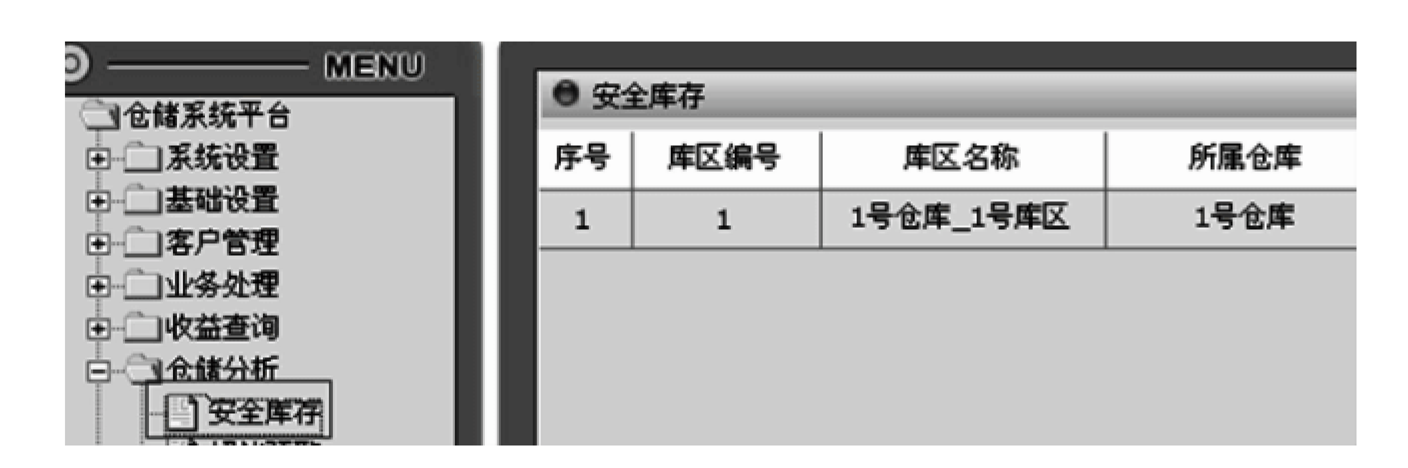


图 8.25　安全库存信息

② 超储预警。超储预警是查询库区使用比例在 60%以上的库区情况，单击左框架“仓储分析”下拉列表中的“超储预警”，即可查看超储预警信息(这里没有超储的库区)。

③ 低储预警。低储预警是查询库区使用比例在 10%以下的库区情况，单击左框架“仓储分析”下拉列表中的“低储预警”，即可查看低储预警信息。

④ 统计分析。统计分析是对以上三种情况的柱状图显示。单击左框架“仓储分析”下拉列表中的“统计分析”，即可查看统计信息，如图 8.26 所示。

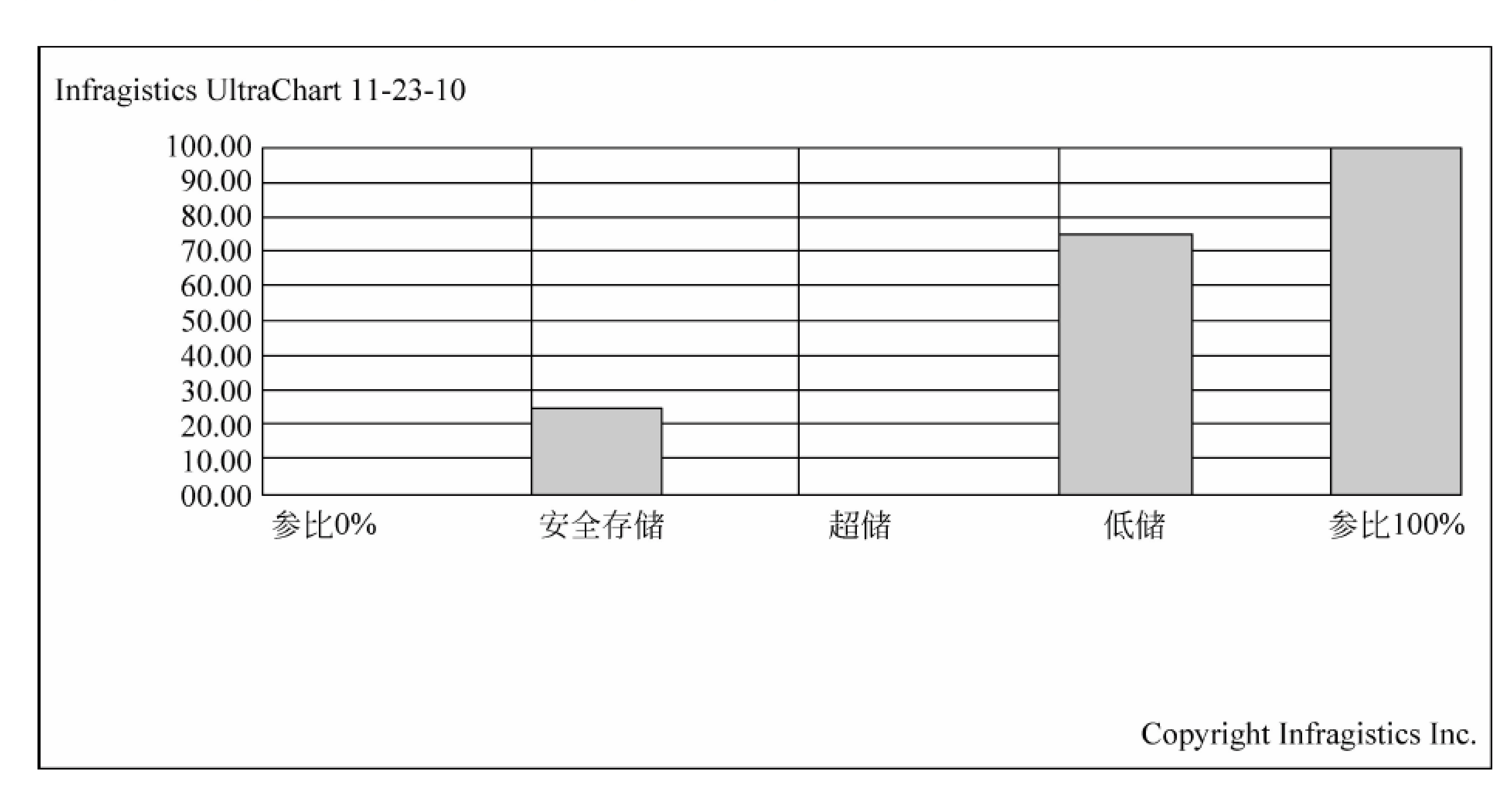


图 8.26　统计信息

（3）库龄分析：主要是查询仓库库区的年限，可分为按年分析和按月分析两种。

① 按年分析。单击左框架“库龄分析”下拉列表中的“按年分析”，在右框架中显示按年分析表，如图 8.27 所示。

Infragistics UltraChart 11-23-10
100.00 90.00 80.00 70.00 60.00 50.00 40.00 30.00 20.00 10.00 00.00
参比0% 1年以内 1～2年 2～3年 3～5年 5年以上 参比100%

图 8.27 按年分析

② 按月分析。单击左框架“库龄分析”下拉列表中的“按月分析”，在右框架中显示按月分析表，如图 8.28 所示。

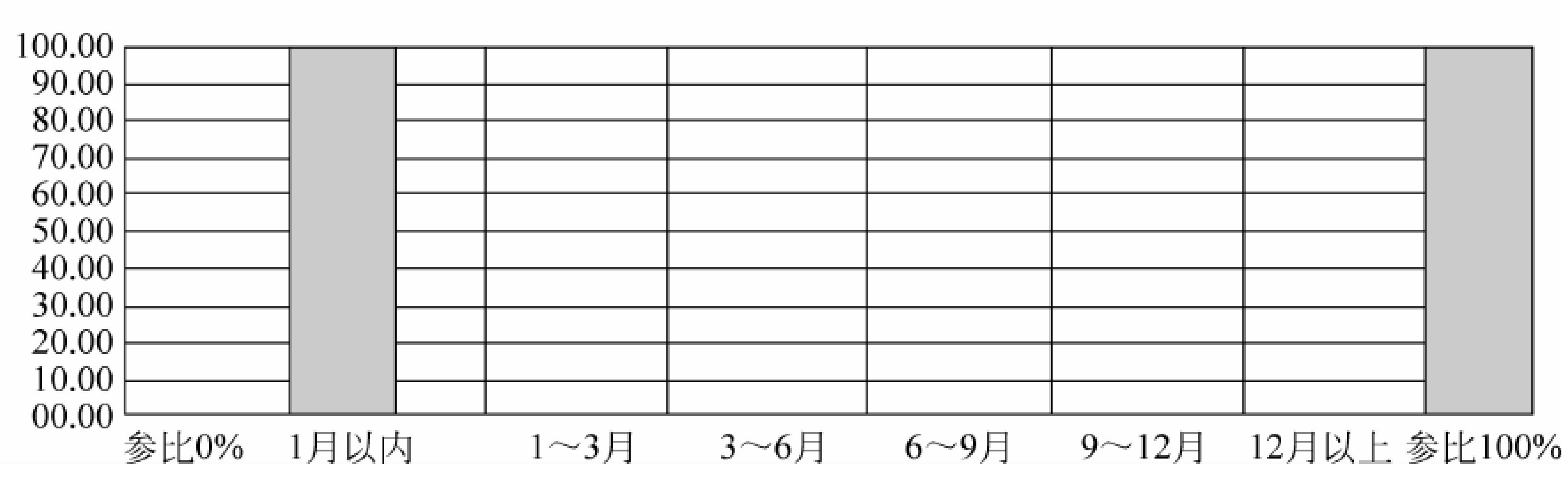


图 8.28 按月分析

8. 思考题

物流仓储如何实现的？

参 考 文 献

[1] 宋文官,等.网络营销.北京:清华大学出版社,2008.
[2] 宋文官,等.电子商务概论.2版.北京:高等教育出版社,2008.
[3] 蔡京玫,等.计算机网络基础实验.北京:中国铁道出版社,2008.
[4] 宋文官,等.仓储与配送管理实务.北京:高等教育出版社,2010.
[5] 冯登国,等.信息安全技术概论.北京:高等教育出版社,2010.
[6] 牛少彰.信息安全导论.北京:国防工业出版社,2010.
[7] 黄传河,等.网络安全防御技术实践教程.北京:清华大学出版社,2010.